ARMY RESEARCH LABORATORY

Analyzing Threats to Army Tactical Internet Systems

by Robert L. Haworth

ARL-CR-423 October 1998

prepared by

MITRE Corporation
1820 Dolley Madison Boulevard
ATTN: Dept G045, MS W-967
McLean, VA 22102-3481

under contract

DAAB07-98-C-E601

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory
Aberdeen Proving Ground, MD 21010-5423

ARL-CR-423 **October 1998**

Analyzing Threats to Army Tactical Internet Systems

Robert L. Haworth
MITRE Corporation

prepared by

MITRE Corporation
1820 Dolley Madison Boulevard
ATTN: Dept G045, MS W-967
McLean, VA 22102-3481

under contract

DAAB07-98-C-E601

Abstract

The risk faced by the Army Tactical Internet (ATI) is a function of four elements: vulnerabilities, threats, operational impact, and safeguards (countermeasures). It is clear that the vulnerability of the U.S. information infrastructure is growing more acute. Not only are more activities becoming dependent on information systems, but these information systems are becoming more open to outsiders and, in the process, adopting technologies that make them less secure. Security technologies are themselves advancing, but the sophistication, availability, and ease of use of hacker tools is advancing faster. The consequences of any attack on the ATI include the *compromise of* information, *deception,* and *denial/loss.* Impact is determined by the operational context in which the damage occurs. The degree of potential damage to ATI systems will guide operational users, in conjunction with materiel developers, in selecting appropriate safeguards. The number and type(s) of safeguards employed should balance operational integrity, systems security, and cost concerns in a risk-managed environment.

Preface

The MITRE Corporation produced this report by direction of, and funded by, the Survivability/Lethality Analysis Directorate, U.S. Army Research Laboratory (ARL/SLAD). The Government Project Director was Mr. Edward Panuska (Information Operations (IO) and Command, Control, Communications, Computers, and Intelligence (C4I) Mission Area Manager). Project Coordinator was Mr. Rick zum Brunnen (Non-C4I System Leader, Information Operations and C4I Branch).

Analyzing Threats to Army Tactical Internet Systems is a revision of an unpublished MITRE Technical Report (*Army Tactical Internet Systems: Threat Analysis*) which was originally distributed as a working draft within the Army Research Laboratory (ARL) in October 1996. The revised draft has been thoroughly reorganized and updated with information current as of 15 April 1998. Its purpose is to acquaint the nonspecialist with the prevalence and magnitude of threats to modern automated information systems such as those making up the Army Tactical Internet (ATI). Only if the relevant fiscal, program management, and user communities are sensitized to the existence of such potential threats can they make rational and prudent decisions with regard to the process of securing ATI systems.

INTENTIONALLY LEFT BLANK.

Contents

List of Figures

List of Tables

INTENTIONALLY LEFT BLANK.

1. Introduction

1.1 Background

Having sufficient, correct information available when needed has always contributed substantially to the success of military operations. Never has this been more true than today, when armies find they must exploit the tremendous advantages inherent in the seamless information-sharing offered by computer and digital networking technologies if they wish to remain among the first (or even second) rank of military powers.

As the U.S. Army's information needs have grown to support success in warfighting, its reliance on automated information assets has likewise grown. Army information systems have become highly interconnected. However, such interconnection has also increased access to those systems by potential attackers—notably via the public Internet. The benefits of increased connectivity are thus partially offset by the increased vulnerability such connectivity presents to various types of attacks.

1.2 Scope and Approach

This report presents a summary of the threats presented to Army tactical information systems. In particular, it is intended to document the serious threat, which organized and motivated *remote attackers* pose to Army Tactical Internet (ATI) systems.[1]

For the purposes of this report, ATI *systems* are distinguished from the ATI itself. Threats that are unique to the ATI *as a network* are not specifically addressed herein, although the unique threats that face networks are in addition to those that face its component systems.

Finally, due to the wide variety and constantly evolving nature of the system configurations involved, this report does not address *implementation-specific* vulnerabilities in ATI systems and networks. Rather, the approach taken here is to identify vulnerabilities presented by the very nature of the ATI and the environment in which it functions, then attempt to outline a risk-assessment process.

This report is a revision of an unpublished MITRE Technical Report, *Army Tactical Internet Systems: Threat Analysis*, originally distributed as a working draft within the U.S. Army Research Laboratory (ARL) in October 1996. The revised draft has been thoroughly reorganized and updated with information current as of 15 May 1998.

The information contained in this report was gathered exclusively from publicly available sources. Complete references are provided.

---

[1] This is to say nothing of the other categories of national security systems at risk. For example, while the software that maintains banking and medical records, guides automated manufacturing processes, and controls critical infrastructure is not usually thought of as a "military asset," its continued security has come to represent part of the definition of "victory" in a future information war.

1.3 Organization

Section 2 describes the various components of the ATI architecture, the Army's plans for using the network on the 21st Century digitized battlefield, and the ATI's place within the context of higher- and lower-echelon Army command and control (C2) systems and standards.

Section 3 discusses the vulnerabilities of routers[2] and hosts[3] in general, various threats potentially posed to the ATI, and the risks to ATI functionality associated with each type of threat.

Section 4 presents MITRE's conclusions and recommendations.

---

[2] A *router* is a special-purpose computer (or software package) that handles the connection between two or more networks.

[3] *Hosts* are the communicating systems that make up a computer network.

2. The Army Tactical Internet and Related Systems

2.1 The Army Tactical Internet: Description and Concept

The ATI is a developmental, integrated communications system that is intended to move unprecedented amounts of information on the demanding tactical battlefield of the early 21st Century. Commercial Internet technology, such as routers, and standards, such as the Transmission Control Protocol (TCP) and the Internet Protocol (IP), is the key to providing seamless connectivity within and between tactical units.

The ATI will be an integral part of Force XXI—the name given to America's near-term digitized Army. It is thus an essential part of the Army's effort to capture the benefits of the Revolution in Military Affairs (RMA)—to build what former Chairman of the Joint Chiefs of Staff Admiral William Owens, Ret., likes to call a "system of systems." Force XXI will be built on the Army's ability to exploit command, control, communications, computers, and intelligence (C4I). The ultimate product Force XXI will be Army XXI—the fully digitized 21st Century Army, which is expected to emerge after the year 2010. The Army intends to field its first digitized division in the year 2000, and a digitized corps by 2004 [1].

A conceptual overview of the emerging ATI is shown in Figure 1. The paragraphs that follow review the Army's plans for the ATI and describe its components—both those being tested now and those likely to be implemented within the next several years.

Soon after the turn of the 21st Century, three legacy tactical communications systems—the Enhanced Position Location Reporting System (EPLRS), the Single Channel Ground-Air Radio System (SINCGARS), and the Mobile Subscriber Equipment/Tactical Packet Network (MSE/TPN)—will be combined to form a complete, seamless communications system that will provide the tactical equivalent of commercial Internet architecture for digitized brigades, divisions, and corps. The Army will tie these three legacy systems together using widely accepted protocols for information processing and transport, such as the TCP and IP. A tactical router called the Internet Controller (INC) is also under development. The local area networks (LANs) operating within each Tactical Operations Center (TOC) in the digitized brigade, division, and corps can also be considered to be part of the ATI. Near-Term Digital Radio (NTDR) is expected to be a part of the first digitized division.

Army leaders intend the ATI and its component systems to revolutionize the way information is collected, processed, and distributed on the battlefield. The revolutionary potential of the ATI becomes clear when one examines the way the Army has been used to doing business in the past, as far as tactical communications and data sharing are concerned. In nondigitized Army maneuver units, reporting methods are serial, manual, and time-consuming. Spot Reports are passed upward from the lowest tactical level by voice radio—when a brief pause in the close-in battle allows time to forward the report. The information is received by a radio operator at the next echelon, who hand-copies it and aggregates it with other reports being received at the same time. He, in turn, retransmits the information to his next-higher command echelon as time permits.

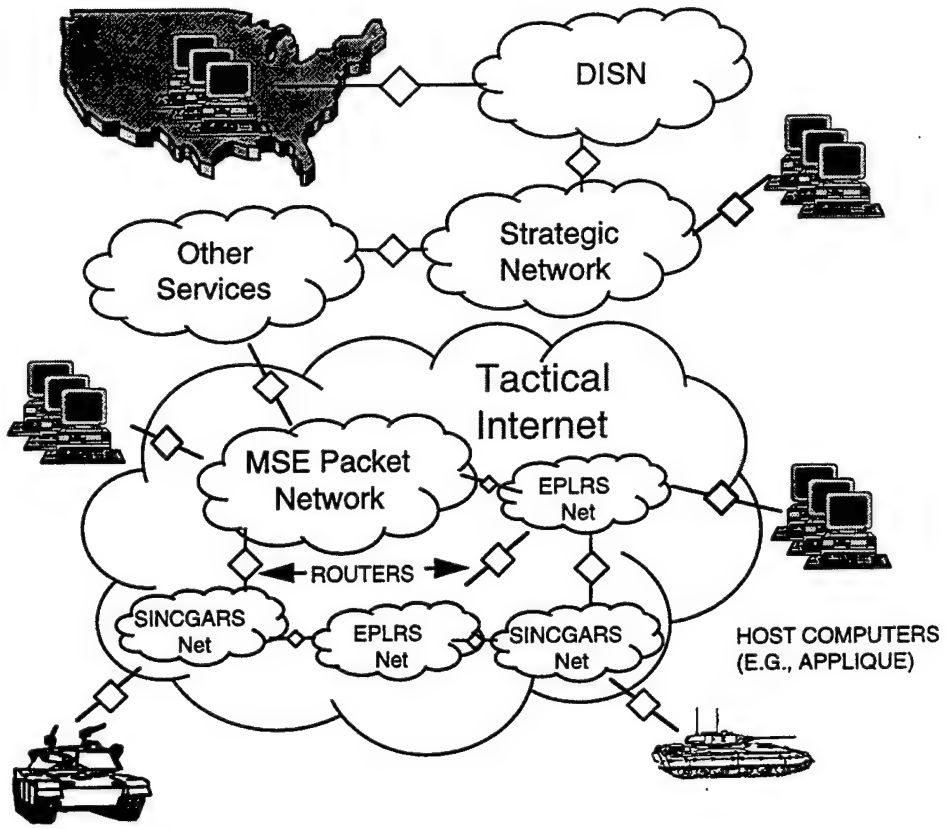

Figure 1. The Army Tactical Internet.

This laborious process is repeated at each succeeding level; the information gradually climbs the hierarchical structure of the Army communications net (which parallels the pyramidal, layered organization of the Army command). Not surprisingly, the time lag involved in the end-to-end transmission of even a simple Spot Report can be significant. *Ad hoc* attempts on the part of enterprising commanders and soldiers to pass information *laterally* within the current command structure, or from one battlefield operating system (BOS) to another, are typically hit or miss.

The ATI is meant to change this picture completely. The concept of *information sharing* is key to the ATI vision. Information will, in theory, be readily available to every authorized user with access to the network. Such connectivity will dramatically decrease the time needed to convert a decision into execution, whether that decision is communicated via a fragmentary order (FRAGO) appearing on the recipient's Graphic Display Unit, or by means of a hasty, "John Madden"-type operations sketch electronically overlaid on his digital terrain map. The ATI will also interface with commercial and military satellite communications (SATCOM) systems, in order to provide Army small units with the amount, currency, and quality of information previously available only at much higher echelons. The fusion of superior information, gathered by multispectral sensors, with efficient information-management systems will enable U.S. units to sustain a faster tempo of operations than the enemy, which in turn should allow U.S.

commanders to "get inside" the enemy's decision cycle. By staying at least one step ahead of the enemy, we should be able to concentrate mass (or fire) on him at the decisive point.[4]

Perhaps most important, the ATI promotes shared *situational awareness* (SA) among tactical forces. Shared SA means that all friendly parties—commanders and subordinates—have a common understanding of the battlespace, as well as the ability to rapidly and clearly communicate information and orders. By using the satellite-based military Global Positioning System (GPS), Army units at all levels locate their current positions to accuracies as close as one meter. The GPS reading is automatically communicated by radio up-echelon to the Maneuver Control System (MCS), located at a TOC. This device assembles the Friendly portion of the common operational picture. As the Friendly portion is updated, so too intelligence about the enemy situation is rapidly fused, analyzed, and transmitted. Enemy icons appear on all units' common visual display.

Shared SA information provides every ATI user with the same, near-real-time picture of the battlespace. By accessing a distributed database, a digitized division headquarters can ascertain the current location and status of *any one* of its subordinate vehicles! Shared SA information means that maneuver operations can be more tightly synchronized—while instances of fratricide can, in theory, be greatly reduced.

As shown in Figure 2, the ATI supports shared SA by employing SINCGARS radios at the platoon level. The backbone of the communications system linking platoons with their parent company and to battalion is the EPLRS Carrier Sense Multiple Access (CSMA) radio. The EPLRS Multisource Group (MSG) provides a data link between battalion and brigade.

Unlike the commercial Internet—an aggregation of over 75,000 other networks (including almost 30 million hosts) in more than 125 countries—the ATI will be SECRET system high; therefore, direct connections to the unclassified, commercial Internet cannot be permitted.[5] The Army has, however, shown great interest in procuring end-to-end encryption devices that will permit ATI users to access the Unclassified (but Sensitive) Internet Protocol Routing Network (NIPRNET). NIPRNET is, however, connected via gateways[6] to the commercial Internet. As a result, all Force XXI networks will be connected *indirectly* to the "outside," and thus may potentially be subject to attacks originating anywhere in the world.

The developmental ATI got its first real test during 1997 in a series of two Advanced Warfighting Experiments (AWEs), sponsored by the Army's Battle Laboratory Program. The objective of the AWEs was to determine the ways in which Army doctrine, training, and/or organization should change in response to the new technology. The first large-scale Force XXI AWE was held in March 1997 at the National Training Center (NTC), Fort Irwin, CA. During this field training exercise (FTX), called *Task Force XXI,* the Army's first digitized

---

[4] The Army's operational concept for Force XXI is spelled out in Refs. 2 and 3.

[5] The sheer number of machines connected to the commercial Internet provides a smart attacker with a great degree of cover for his actions. Most of the world has either direct or dial-in connectivity to the Internet, typically within their own country's national boundaries.

[6] A *gateway* is a computer that controls data communications between a LAN and a wide-area network (WAN).

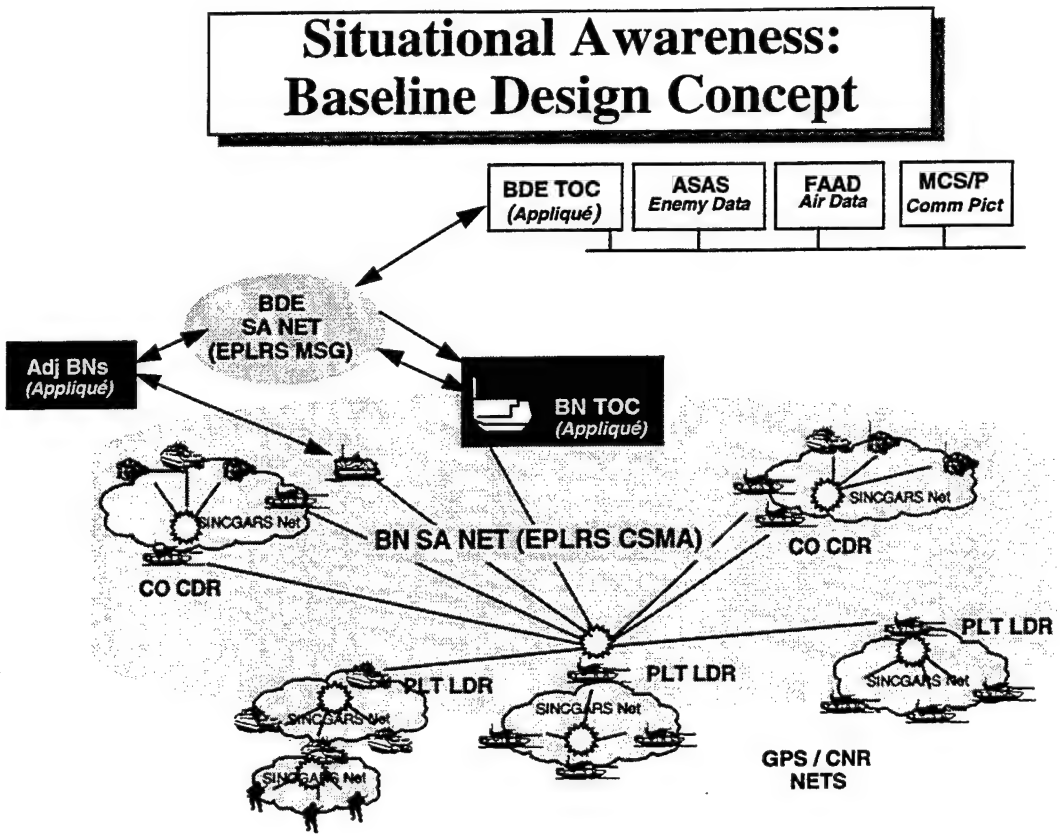

Figure 2. Promoting Shared Situational Awareness.

brigade[7] fought a conventionally armed opposing force (OPFOR). Some 72 new Force XXI technologies and initiatives were tried out during the week-long AWE, with mixed results. On the one hand, the Experimental Force (EXFOR) took less time to plan missions than the average nondigitized U.S. brigade; command and control were "tighter" and more sure. On the negative side, there were a number of technical problems: one result of these was that EXFOR experienced a high level of fratricide.[8]

The ATI was tested again as part of a division-sized command post exercise (CPX), *Division XXI*, held at Fort Hood, TX, in November 1997. This time, the configuration of the ATI was more stable and its operators more experienced. These factors resulted in a better showing for the ATI.

---

[7] First Brigade, 4th Infantry Division (Mechanized).

[8] Computers crashed because they were overloaded and/or were exposed to the pervasive dust of the desert. The sky over Fort Irwin was so full of electronic communications that conventional radio messages sometimes could not get through. Technical bugs undermined soldiers' confidence in the currency of the enemy situation information supplied to them. EXFOR was judged to have suffered three times the friendly fire casualties normally expected in a brigade exercise (Ref. 4).

2.2 The Future of the ATI

Army planners anticipate that by about 2002, an ATI based on legacy systems will be unable to handle enough data traffic to function effectively. To handle the shortfall, the Army plans to replace EPLRS and SINCGARS first with a NTDR and, ultimately, with a more capable Future Digital Radio (FDR). It will also replace MSE/TPN with a system called the Warfighter Network, Terrestrial (WIN-T) in at least the first digitized division. WIN-T incorporates Asynchronous Transfer Mode (ATM) technology, which can transmit imagery.

The Army also wants a wireless capability to pass graphic overlays and SA reports, as well as real-time video teleconferencing. To accomplish this, it is also considering low-earth-orbit (LEO) and Direct-Broadcast Satellite (DBS) systems. The latter is considered especially well-suited for live video transmission to the ATI and will be incorporated in the first digitized division.[9]

Finally, there may be follow-ons to the Internet Controller and/or to TCP/IP itself as the backbone data transmission protocol set. At a minimum, the current version of IP (Version 4) will probably be replaced with Version 6 [6]. IP Version 6 (IPv6) enables much greater flexibility in addressing than does IPv4; it also incorporates significant security features, with an emphasis on nonrepudiation.[10]

The next-generation ATI is expected to evolve by around 2010. Due to the exceptionally rapid and relentless advance of computing and communications technologies, however, no one can at present say for certain just what it will look like. Special intelligence and indications and warning (I&W) information may be provided to the ATI via satellites in geosynchronous orbit, such as the U.S. Military Strategic and Tactical Relay Satellite System (MILSTAR). The addition of wideband, high-frequency (HF) radios to the ATI may extend its "sensing range" considerably; long-range surveillance units with manpack high-frequency (MHF) and other HF radios should be able to communicate directly with the ATI [5, p. 65].

2.3 ATI-Related Systems and Standards

A number of systems serve the Army's C3 needs at echelons higher than, and parallel to, the tactical level at which the ATI operates. It is important to know something about these systems since, as suggested earlier by Figure 1, future Army, interservice, and strategic-level C3 is intended to be carried on in a more or less completely networked environment. Unfortunately, networking by its nature potentially exposes the network as a whole—and each of its component systems—to the security weaknesses of any one component.

---

[9] For the 1997 AWEs, a Battlefield Awareness Data Dissemination (BADD) terminal was provided at selected TOCs to allow the downloading of intelligence information from DBS. However, it is by no means certain that a DBS capability will be part of the ATI when the latter reaches final form. Ref. 5, p. 64.

[10] IPv6 is currently in development; significant commercial implementations of the completed international standard are expected to appear as early as mid-1999. For a summary of the differences between IPv4 and IPv6, see Refs. 7 and 8.

2.3.1 The Army Battle Command System (ABCS)

The ABCS is an automated battlefield management system that is intended to provide seamless C3 from the strategic echelon to the foxhole. The ABCS satisfies two critical requirements in support of C3 planning and execution for the tactical commander. First, it provides a common picture of the battlespace, promoting SA. A new generation of satellites and unmanned aerial vehicles (UAVs) will eventually provide unprecedented real-time intelligence via the ABCS, which will process and disseminate relevant data over the ATI [5]. Second, it will ensure the interoperability of the BOS: the ABCS will support the automatic entry of inputs received from the various BOS connected to it (including their location and status).

The ABCS has three main components:

- The Global Command and Control System, Army (GCCS-A).
- The Army Tactical Command and Control System (ATCCS).
- The Force XXI Battle Command Brigade-and-Below (FBCB2) Appliqué.

2.3.1.1 The GCCS-A

The GCCS-A, itself a subset of the U.S. national-level Global Command and Control System (GCCS), will be used by Army commanders at the theater and strategic echelons. It is therefore interoperable with other high-level joint and combined U.S. command systems.[11]

2.3.1.2 The ATCCS

ATCCS will be the Army's C3 system serving intermediate echelons, from corps down to battalion. It will be used by commanders at these echelons to analyze rapidly evolving combat situations, including friendly and enemy capabilities, to determine U.S. information and materiel requirements, to develop courses of action, and to disseminate the commander's intent and orders. The five primary components of the ATCCS are shown in Figure 3.

The following paragraphs describe the roles and missions of the five ATCCSs that were employed in the 1997 AWEs.

The Air and Missile Defense Workstation (AMDWS).[12] The AMDWS not only develops the common air picture but also has an engagement operations capability in its air defense role.

The All-Source Analysis System Remote Workstation (ASAS-RWS). The ASAS-RWS collects, analyzes, maintains, and distributes enemy situation data that are relevant to each land component echelon from corps through battalion. Its primary mission is to maintain the Enemy

---

[11] GCCS-A includes all of the capabilities previously provided by the Standard Theater Army Command and Control System (STACCS), the Army Worldwide Military Command and Control System (WWMCCS), the Army WWMCCS Information System (AWIS), and the echelons-above-corps portion of the Combat Service Support Control System (CSSCS).

[12] Follow-on to the Forward Area Air Defense Command, Control, Communications, and Intelligence (FAADC3I) system, the AMDWS is currently under development and will be procured beginning in 2002. See Ref. 9.

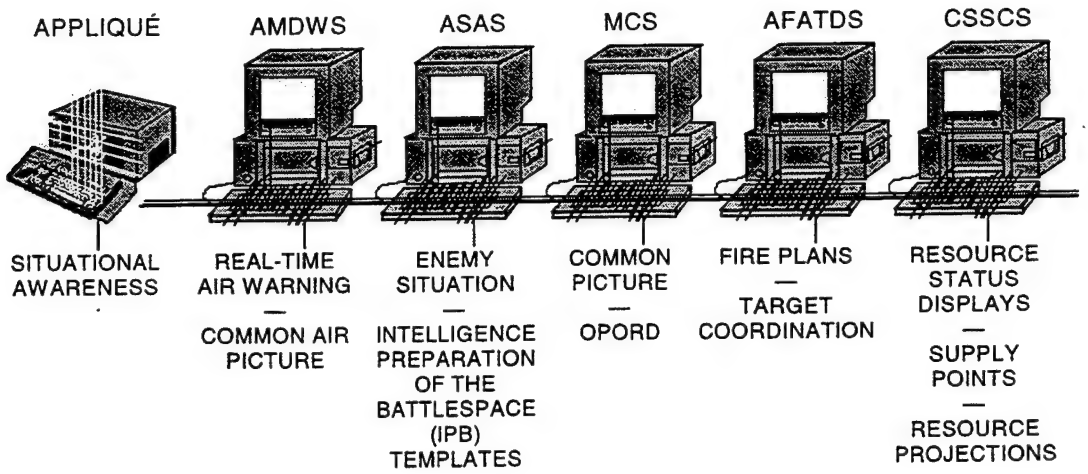

Figure 3. Roles and Missions of the ATCCS' Primary Components.

portion of the *common operational picture* (COP)[13] at each echelon, including the intelligence sections of the operations order (OPORD) and the enemy overlay.

The MCS. The MCS assembles and distributes a COP based on a view of the current situation *one echelon up and two echelons down* from the point of view of the relevant tactical commander/"owner." That is, a brigade commander can expect a COP showing the military situation, *relevant to him,* as it is known to exist by echelons ranging from division, directly above him, to company (two echelons below). Operational overlays include the Friendly and Enemy situations, the current status of fire support, air defense, logistics planning and execution, and the notional geometry of the battlefield (e.g., unit boundaries and phase lines).

The Army Field Artillery Tactical Data System (AFATDS). The AFATDS develops and maintains the Friendly fire support portion of the COP and has an engagement operations capability.

The CSSCS. The CSSCS develops and maintains logistics readiness data for the commander and provides resource data to the MCS to allow the commander an overview of unit readiness. The CSSCS also maintains a Unit Task Organization Server and a Reports Server; together, they provide access to the detailed resource information needed by Personnel (G1/S1) and Logistics (G4/S4) officers on a battle staff, and to other ATCCS subscribers.

Three other C3-related digitized systems are planned to work in cooperation with ATCCS but have not yet been tested in an AWE. These are the Integrated Meteorological System (IMETS),

---

[13] The COP crosses horizontal, vertical, and functional boundaries. Automated update mechanisms provide the following:

- Situation maps and overlays (including friendly and enemy situations, fire support, air defense, and logistics planning and execution).
- Summary-level resource reports from the Commander's Tracked Items List (CTIL).
- Operation plans and orders.
- Updated unit task organizations (UTO).

the Aviation Mission Planning System (AMPS), and the Automated Nuclear/Biological Information System (ANBACIS).

2.3.1.3 The FBCB2 Appliqué

All vehicles in the Army's first digitized division will contain add-on, ruggedized personal computers of at least the 80486 generation (called *Appliqué*). The Appliqué screen displays friendly and enemy units as icons. Different icon shapes and colors distinguish each unit by side (enemy or friendly), unit type, and status (alive or "dead").

Appliqué provides automated C3 and SA information for all Army elements at brigade and below that currently do not have access to ATCCS and its associated COP capability.[14] Appliqué provides message processing for these elements and collects and disseminates engagement data (location, fire support, and intelligence) for all platforms subordinate to the brigade. Appliqué also provides air track warning alerts and resource inputs to the CSSCS. Finally, Appliqué provides a communications gateway: messages (in Variable Message Format [VMF]) are exchanged between ATCCS hosts and remote Appliqué units for those ATCCSs that do not have the ability to connect directly to the ATI. The "core" of FBCB2 is its *Embedded Battle Command* (EBC) software.

Standards that must be considered part of the context of Army XXI C3 are the Defense Information Infrastructure Common Operating Environment (DII COE) and the Joint Technical Architecture-Army (JTA-A) and Joint Technical Architecture (JTA), respectively.[15]

The ATI initiative has changed the face of Army C3I for good. The new technologies, tactics, techniques, and procedures that are being counted upon to make the ATI work also make necessary a new assessment of the threats posed to the ATI.

---

[14] At the two AWEs held so far, only one of every three combat vehicles, on average, has had an ATCCS host installed; the other two-thirds had Appliqué only.

[15] See Ref. 10 for the text of the JTA-A; Ref. 11 for the text of the JTA.

3. Identifying and Evaluating Threats

3.1 Elements of Risk

The *risk* faced by the ATI is a function of four elements:

- The existence of technical and procedural *vulnerabilities* in our networks and computing systems. A vulnerability is defined as a system weakness that could allow security to be violated.
- The presence of a *threat*. Threats are entities, events, or circumstances that could cause harm by violating security. Threats most often exploit vulnerabilities.
- The *impact* resulting from the loss of critical information, systems, or network(s). Impact is the damaging effect exerted on an asset (here, the information and/or availability of the ATI) by a threat.
- The *safeguards* (countermeasures) available. Safeguards are techniques, procedures, or devices that make a threat(s) weaker or less likely.

Where vulnerabilities are numerous, the threat significant, the impact of a data or equipment loss high, and safeguards limited, risk to a system or network is obviously extreme.[16] Unfortunately, all of these conditions are present in the current ATI environment. The next section presents a step-by-step framework that can be used to help make decisions about the relative commitment of resources needed to reduce risks to ATI systems to an acceptable level.

3.2 Vulnerabilities

3.2.1 Understanding the Networked Environment

U.S. Army formations having access to the ATI and its related computing and communications systems enjoy a significant technological advantage over potential enemies. The United States has continued to advance the state of the art in using networked automated systems to improve the tactical and operational effectiveness of its military forces. In Force XXI, the interconnection of all assets will be greatly increased in an effort to improve SA.

However, as the battlefield is digitized, security has become an issue. The U.S. Army Digitization Office's *Army Digitization Master Plan* states that "...the infusion of information age technology into the Force XXI battlespace has increased the vulnerabilities of our information systems and created a more complex scenario for protecting the information distributed through [it] [13]. Expansion of automation devices in weapon systems and command-control; the increased networking of those devices for improved horizontal and vertical connectivity; and the tremendous increase in supporting data communications have brought about a commensurate increase in protection requirements [14]." The *Master Plan* reflects the fact that the technology and procedures employed to guarantee the security of Force XXI information are at least as important as the integration of the technology that makes sharing that information possible.

---

[16] This calculus of risk is found in Ref. 12, pp. 2-17 and 2-18.

When operationally deployed, Force XXI networks will utilize end to end encryption to maintain connectivity with the NIPRNET, which is, in turn, connected via gateways to the public Internet. In addition, most U.S. military networks depend upon the commercial sector to transmit messages and to provide infrastructure support. The Army's reliance upon commercial infrastructures, both domestic and foreign, for transmission and processing of telecommunication and information services is currently estimated at over 90 percent, and is anticipated to increase in the mid-term [14]. The systems, assemblies, and subassemblies making up these commercial networks continue to be developed with limited regard to their individual or collective vulnerability to computer network attack. The use of commercial communications assets "...presents the greatest challenge to information availability and reliability, because the deployed force commander no longer controls circuit availability, reconfiguration, or reconstitution [14]."

3.2.2 General Types of Vulnerabilities [15]

- *Authentication-based* vulnerabilities are those that permit someone to falsely assume the privileges of a legitimate user. Authentication mechanisms are vulnerable to password sniffing/cracking, "social engineering"[17], and access via another already corrupted, yet trusted, system.
- *Software-based* vulnerabilities are such things as viruses, excessive user privileges, "back doors," and poor system configuration—the latter often involving unused security features.
- *Protocol-based* vulnerabilities include easily guessed IP sequence numbers and unused header fields.
- *Data-driven* vulnerabilities include the ability to direct electronic mail (e-mail) messages to an application program, embedded programming languages (i.e., the MS Word "Concept Virus"), and a number of other esoteric vulnerabilities having to do with mobile code systems (such as Java and Active-X).
- Vulnerabilities resulting in *denial of service*—wherein legitimate users are prevented from using the network—include flooding[18], and the Morris "Internet Worm" of 1988.
- *Human frailty* accounts for what are probably the most pervasive, yet most easily preventable, computer vulnerabilities. Humans too often make poor password choices,

---

[17] *Social engineering* is a slang term referring to a human intelligence function used to support analysis of configuration data, organizational relationships, and the location of critical information nodes (including key personnel). It can be employed to support computer network attack and/or psychological operations, and to defeat operational and physical security measures. Perhaps its most common use by the computer hacker is to trick people who know secrets connected with computer systems—passwords, for example—into revealing them. For example, a hacker might place a telephone call to a harried system administrator in a large company, claiming to be an executive who has forgotten his or her password.

[18] *Flooding* occurs when a user prevents a system from processing its normal workload by directing a large number of network messages to that system, such that the target devotes most of its resources to responding to the messages. In extreme cases, flooding may so stress a system's available memory and/or cause so many processing errors that the system crashes (as in the "ping of death" attack), resulting in denial of service. Flooding attacks directed against one machine can also mask an attack on another, by preventing audit records from being processed in a timely manner.

allow insecure system configurations to persist, and are taken in by the ploys of "social engineers."

3.2.3 Sample Vulnerabilities of Hosts and Routers

Samples of the vulnerabilities of hosts and routers such as those which make up the ATI are shown below. These lists are not exhaustive; they serve instead as a useful guide for further work in assessing the threat against the specific hosts and routers that make up the ATI. Acknowledgment of the vulnerabilities inherent in the "building blocks" of the ATI—its hosts and routers—serves as a starting point for a methodical assessment of the security posture of the network as a whole.

3.2.3.1 Host Vulnerabilities

The typical consequences of attacks that exploit host vulnerabilities are summarized (by Open Systems Interconnection [OSI] Model Layer)[19] in Table 1.

3.2.3.1.1 Application Layer.

- **Null Shell Field**: No default shell is specified for a log-in account—unauthorized users can easily log in.
- **World-Writeable System Files**: A configuration that allows any user to modify sensitive system-configuration files.
- **Duplicate User Identifiers (UIDs)**: An administrative error in which the same UID is assigned to two or more users. Any such user can then access the files of his colleagues having the same UID.
- **Sendmail**: A wide variety of vulnerabilities are known to exist in standard e-mail software utilities, such as UNIX *Sendmail*.
- **The Network File System (NFS)**: Allows remote mounting of file systems and is easily misconfigured, allowing unintended access to the exported file systems. In the most common exploitation of this vulnerability, unauthorized persons use the commercial Internet to export an NFS file system to their own machine.
- **User-to-User Decode (UUDECODE)**: Invoked via *Sendmail*, UUDECODE can be used to create arbitrary Superuser IDs (SUIDs), allowing unauthorized persons to execute commands with "root" privilege.
- **Trivial File Transfer Protocol (TFTP)**: Misconfiguration may allow both read-and-write access to all TFTP-accessible files and directories, without password authentication.
- **Anonymous File Transfer Protocol (FTP)**: This configuration error permits anonymous, remote users to retrieve or modify sensitive system files, such as the system's password file.

---

[19] The OSI Model groups the functions and protocols necessary to conduct computer communications into seven layers: Application, Presentation, Session, Transport, Network, Data Link, and Physical.

- **Network Information Service (NIS)**: Manages files belonging to a *domain* of computers; its password files may be stolen and subjected to off-line cracking attempts. Current implementations of NIS present several unfixable security problems. Although it is not a trivial matter to circumvent the controls built into the NIS, neither is it difficult for an experienced programmer having access to certain manuals. Given superuser (unrestricted) access to a local machine, the task becomes much simpler.
- **The X-Windows System**: Unauthorized users can establish access via the commercial Internet, then covertly capture user keystrokes, mouse commands, and the user's monitor display. Such users can take over control of the mouse or keyboard, send keystrokes to other applications, or even kill windows associated with the legitimate user's applications at will.

3.2.3.1.2 Network Layer. Internet Control Message protocol (ICMP) Redirect messages sent to a host by an intruder may cause that host to crash.

3.2.3.1.3 Physical Layer. Attacks on ATI system hosts can include electromagnetic disruption and the use of directed-energy weapons, such as lasers and radio-frequency emitters.

Table 1. Sample Host Vulnerabilities

OSI MODEL LAYER	VULNERABILITY	CONSEQUENCES OF ATTACK
Application	Null Shell Field World-Writeable File Systems Duplicate User IDs Sendmail NFS UUDECODE TFTP FTP NIS X-Windows System	Host Penetration: Provides a platform for launching a network attack
Network	ICMP Redirect	Denial of service
Physical	Jamming Directed Energy	Denial of service Denial of service

3.2.3.2 Router Vulnerabilities

The typical consequences of attacks that exploit router vulnerabilities are summarized (by OSI Model Layer) in Table 2.

3.2.3.2.1 Application Layer.

- **Flaming**[20]
- **Spamming**[21]
- **TFTP**: Router configuration may be modified so as to send system files to an unauthorized destination.
- **TELNET (Telecommunications Network) Service**: The password of the router manager may be stolen by remote log in.
- **Simple Network Management Protocol (SNMP)**: Information may be gathered about a router, which allows an attacker to modify that router's configuration.

3.2.3.2.2 Network Layer.

- **IP**: The originator of an illegal packet or session may misrepresent himself as a legitimate user (AKA "IP spoofing").
- **Access Control List**: An improperly configured access control list may permit unauthorized traffic through the router.
- **Terminal Access Controller Access Control System (TACACS)**: If TACACS is bypassed, an unauthorized user could gain access to the router.
- **ICMP**: An illegal host purporting to be a router may be able to send an ICMP *gateway redirect message* to another router, allowing messages to be sent to the illegal host.
- **IP Fragmentation**: IP fragments may be used to bypass the router's filtering mechanism.
- **IP Source Routing**: Altering IP source routing may allow prohibited communications.
- **Routing Information Protocol**: A router may accept bogus routing information.
- **Open-Shortest-Path-First (OSPF)**: A router may temporarily accept bogus routing instructions.
- **Address Resolution Protocol**: A router may be deceived as to the actual addresses of local hosts or other routers, with the result that the system may send messages to unauthorized hosts.

---

[20] *Flaming* is a slang term referring to the exchange of electronic messages devoted to personal criticism or complaint. *Flame wars* are overheated, multilateral affairs that can degrade the performance of a computer network and consume vast amounts of users' time.

[21] Spamming is a slang term referring to an inappropriate attempt to use a networked communications ("narrowcast") capability as if it was a broadcast medium, by sending the same message to a large number of people who didn't ask for it (as, junk e-mail). USENET and a number of mailing lists on the public Internet are sometimes bogged down by spam.

3.2.3.2.3 Physical Layer. As with physical attacks on hosts, attacks on ATI routers can include conventional jamming, the use of directed-energy weapons, and tapping (the clandestine interception of a link's communications by physical or electronic means).

Table 2. Sample Router Vulnerabilities

OSI MODEL LAYER	VULNERABILITY	CONSEQUENCES OF ATTACK
Application	Flaming Spamming TFTP TELNET SNMP	Denial of service, degradation of network
Network	IP Spoofing Access Control List TACACS ICMP IP Fragmentation IP Source Routing Routing Information Protocol OSPF Address Resolution Protocol	Unauthorized access, unauthorized modification
Physical	Jamming Directed Energy Tapping	Denial of service Degradation of network Unauthorized access

3.3 Threats

3.3.1 Threats Originating in Authorized Access

The Army expects the networked tactical environment to confer tremendous advantages on its 21st Century forces. However, as the following examples suggest, the availability of so much processing and communications horsepower is not without its problems from a security standpoint. Careless authorized users can inadvertently deny access to ATI system resources (e.g., communications devices, storage media); authorized users who commit fraud, waste, or abuse reduce the efficiency and response time of the system. Other than "steel on target," authorized users who are secretly the agents of an adversary power represent perhaps the most formidable threat to ATI systems—especially if those users have advanced knowledge or "superuser" access privileges.

Three types of harmful user actions are as follows:

3.3.1.1 Browsing

An authorized ATI user might browse data files, removable media, or data residues to obtain information or insight on system operations, users, or vulnerabilities, well beyond his or her need to know.

3.3.1.2 User Error

ATI users might make inadvertent errors that violate security. For example, a user might accidentally mislabel sensitive data as UNCLASSIFIED; important data might be inadvertently overwritten or deleted; or user passwords may be observed by an unauthorized individual. While such user errors may not have been made with the intent to cause damage to ATI systems, they may effectively degrade the security or operational readiness of the ATI and may introduce a vulnerability that an adversary could exploit.

3.3.1.3 Administrator Error

System administrators often make errors when initializing or modifying security parameters (e.g., network routing tables and user authorizations). Additionally, user- or system-level passwords might be only loosely controlled. Failure to apply software "patches" and to make security-enhancing upgrades is all too common.

3.3.2 Threats Originating in Unauthorized Access

Unauthorized access includes attempts by any "outsider"—such as a hacker—to access an ATI system. It also includes attempts by authorized users to access data normally prohibited to them, by bypassing need-to-know restrictions or by exceeding their authorized privileges. Unauthorized access is an inherent threat. The threat of unauthorized access is discussed below with respect to access by allies, neutral parties, and enemy forces.

3.3.2.1 Allies

U.S. allies may try to access ATI data that are beyond that authorized to them by treaties or other standing agreements. Some allied personnel might, in fact, be authorized users who attempt to alter safeguards without approval of the responsible Information Systems Security Officer (ISSO), so that they can conduct activities beyond their need to know. Hostile agents posing as allies might attempt to penetrate the ATI in order to compromise, modify, or delete data; alter software security parameters; or deny service. Finally, an unauthorized user might attempt to use the ATI to penetrate *other* networks or systems.

3.3.2.2 Neutrals

Neutrals may present much the same threat as do allied forces, depending upon the type of access they have to the ATI or its component systems. Some neutral nations have been given authorized connections to an ATI system host. The dynamic nature of the United States' international relationships means that today's neutral nation becomes hostile to us in the future. Even if a neutral remains neutral, a U.S. adversary might enjoy some position of advantage over the neutral that forces it to provide unauthorized access to the ATI or the information it contains. Neutrals may not impose the security controls preferred by the United States on the devices they are using; the United States might not have an oversight capability adequate to ensure that the neutrals' security controls are appropriate and vigilantly maintained. Finally, a "neutral" connection to the ATI may be used by an adversary to launch an attack on ATI systems, *without the knowledge of the neutral.*

3.3.2.3 Enemies

If enemy forces gain access to an ATI router or host, the range of possible adverse actions is huge. This threat does not, in most cases, require physical access to the target router or host; "virtual" access (via a computer network) is sufficient.

3.3.2.3.1 Battle Overrun. As the Army Digitization Office (ADO) *Master Plan* points out, "...enemy possession of [ATI] systems, or other unimpeded access to digital data, can result in severe damage being inflicted on friendly forces [13]." If an ATI system is overrun, the adversary may be able to fully document the ATI's capabilities, or even set up the captured system as an offensive information warfare (IW) workstation. The adversary could use such a workstation to attempt to degrade all ATI systems of that same type or to completely shut down the ATI itself.

3.3.2.3.2 Enemy Objectives. In attacking the ATI (or, indeed, any Army C2 system), an adversary may wish to do the following:

- Obtain access to classified or sensitive military information.
- Sow disinformation.
- Cause the degradation or failure of the system.
- Misdirect U.S. forces, weapons, or sensors.
- Disrupt Army lines of supply.

An adversary acting in pursuit of such mission-oriented objectives will seek to identify and exploit vulnerabilities in the physical, procedural, and automated security systems that protect the ATI and its components. The challenge facing the defender is that he cannot know or protect against all possible means of attack and must thus employ a *risk-management* strategy. However, an attacker potentially needs to know about only one point of weakness in order to succeed, thus the need for resilient systems and robust recovery capabilities.

3.3.2.3.3 Attack Profiles. In assessing risk, it is not sufficient merely to determine the vulnerabilities of a system to specific types of attacks and the probable impact(s) of an actual attack on it. It is also important to identify the motivations and capabilities of the threat—that is, of potential adversaries who might attempt to attack the system—and the general ways in which such adversaries would go about an attack. For the purposes of this assessment, MITRE has identified four *attack profiles* to help characterize computer-based remote attacks.

- An *unfocused* attack is carried out without prior identification of a specific target or attack objective.
- An *unstructured* attack is performed by an individual or loose collection of individuals who intend to launch an attack but have not (yet) committed specific resources and/or capabilities to carry it out.
- A *focused* attack results when the perpetrator(s) pursue a definite objective ("victory condition") by attacks on a specific target(s).
- A *structured* attack is one performed by an organized group that has committed specific resources to carry it out.

This concept yields the four-celled matrix shown in Table 3, wherein each type of attack is briefly characterized.

Table 3. Matrix of Attack Structure vs. Focus

FOCUS		STRUCTURE: No	STRUCTURE: Yes
	No	Individual Mental Challenge Least Threatening	Group Still Organizing Group in Transition Targets of Opportunity
	Yes	"Grudge" Perpetrator Money or Intelligence Targets *.gov* and *.mil*	State Sponsors Can Recruit Talent Most Threatening

Each of the four resulting attack profiles is described in greater detail in the following paragraphs.

Attack Profile 1: Unfocused, Unstructured. This is probably the least-threatening potential attack. It is characterized by a single individual or loosely knit group attempting to penetrate a system without any particular motive other than to serve as a mental challenge or means of recreation. The perpetrators of these attacks sometimes have special expertise in one or more areas of computer or network technology—for example, they might be well-versed in UNIX vulnerabilities that can be exploited over the Internet. If so, they tend to concentrate on targets against which this expertise might help them execute the attack. However, such concentration is incidental and does not represent "focus" for purposes of this analysis.

Attack Profile 2: Unfocused, Structured. This stage is characteristic of computer network attack efforts that have obtained official sponsorship but which are still in the process of organizing themselves. Alternatively, an already well-established effort may be in transition—reorienting itself on a new set of targets from among those presented by the rapidly evolving world computer network environment. Attacks launched by a Profile 2 organization are broad in scope, yet necessarily tentative, and oriented more toward gathering system vulnerabilities and other "research"-type information than toward denying service or inflicting other actual damage.

Attack Profile 3: Focused, Unstructured. The attacker is typically a single individual who is motivated to attack certain types of computer systems (e.g., those belonging to the *.gov* or *.mil* domains on the commercial Internet) but who is operating without the benefit of significant resources or the guidance of an organizational sponsor. Alternatively, the attacker might be an organized group that lacks significant technical or financial resources. While Profile 3 attacks are launched in order to realize some perceived gain—material or otherwise—they do not support any strategic plan. As with Profile 1 attacks, the adversary may have expertise in one or more areas of technology and may therefore direct his attacks against systems which he believes such knowledge might help him penetrate.

Attack Profile 4: Focused, Structured. These attacks, which are carried out by an *organization* that has a specified purpose in attacking, are probably the most threatening to the ATI. The adversary tends to identify a specific subsystem, component, or function as a target, and to establish and stick to a long-range, strategic plan in exploiting it. Usually, Profile 4 attackers are after either money or intelligence. Profile 4 attackers can easily recruit needed

talent and may thus be able, over time, to draw on expertise in many types of systems (including extensive knowledge of system vulnerabilities). The most comprehensively organized are able to develop and execute their own, novel, types of attack.

3.3.2.3.4 Sophisticated and Unsophisticated Attackers. The foregoing analysis suggests that there are two basic attack styles among hackers: unsophisticated and sophisticated. Unsophisticated attackers tend to use high-profile, "brute-force" methods of attack and to exploit well-known vulnerabilities in UNIX and other operating systems or applications. Attacks launched by sophisticated hackers, on the other hand, typically have a much lower profile. These hackers have a great deal of specialized technical knowledge, use multiple attack methods (even employing several methods at once, in simultaneous sessions), and are adept at using route weaving[22] and other methods to cover their tracks—both into and away from the victim system. These attackers can even appear "unsophisticated" when necessary.

It is important to note that a threat may evolve: the Wily Hacker of *Cuckoo's Egg* fame, for example, began his career as a Profile 1 attacker but ended it accepting pay and detailed direction from the Soviet KGB (Profile 4) [16]. En route, he probably transitioned through at least Profile 3. Attack profiles can thus be simultaneously viewed as labels to hang upon generic classes of threat individuals or groups or as potential stages in the "life" of a specific threat.

3.3.2.4 Other Threats

3.3.2.4.1 Malicious Software. Malicious software, such as computer viruses, can be introduced via shrink-wrapped, mass-market commercial software that was manufactured under conditions of lax security, by custom-made software, or by the careless sharing of portable media or public software—though the risk adhering to each of these methods varies significantly. Trojan Horses[23] and worms[24] can be introduced by users, system developers, integrators, or maintenance personnel. Malicious software attacks can cause denial of service, modify or delete data, or alter software security controls. Malicious clients[25] might try to access the contents of ATI objects, relabel classified objects as UNCLASSIFIED, or introduce additional malicious software to spoof legitimate programs and gain information, such as user identifiers and passwords.

3.3.2.4.2 System Failure. This category includes all of the impersonal sources of possible threat to the ATI—most notably natural disasters, random electromagnetic phenomena, and

---

22 *Route weaving* is a technique whereby a computer intrusion is launched across a deliberately very complicated network path, so as to make the accurate and timely tracing of the intrusion to its source host impossible.

23 *Trojan Horses* are programs that, when called by authorized users to perform useful functions, also perform unauthorized ones—such as usurping the privileges of the user or adding "back doors," which hackers can subsequently exploit to get into the system.

24 *Worms* are computer programs that use multitasking to propagate themselves in an out-of-control manner. The resulting consumption of system resources leads to system degradation and, ultimately, to complete denial of service. Worms often spread from computer to computer across network connections. Probably the most famous worm in history was the so-called Morris Internet Worm of 1988. Worms are far less common than their cousins, viruses—probably because writing a successful worm requires far more knowledge and skill.

25 A *client* is any computer that requests a service from another computer, called a *server*, across a network.

everyday equipment malfunction. Classified or sensitive Army data might be lost, modified, or inadequately protected as a result of disk failure, the *Disk Full* or *Memory Full* errors, and failure of access-control mechanisms. Additionally, system recovery procedures might themselves result in a fairly lengthy denial of service. It should be noted that systems undergoing recovery after a crash, and which are still connected to a network, are exceptionally vulnerable to computer network attack.

3.3.3 Computer Network Attack in the Real World

The computerized nature of Third Wave warfare[26]—and the manifest advantages that this war-form conveys on a nation able to practice it—has led many nations to explore the possibility of making attacks against the networks and hosts of potential enemies. A growing number of countries are known to have begun planning to exploit network vulnerabilities for military ends.

First, it is unproductive to try to assess the "technical capability" of any nation to conduct a computer network attack against the ATI. Commercial computer and telecommunications technologies are widely distributed. All nations that are even semideveloped have access to complex and redundant global networks. Even in wartime, it would be very difficult and probably self-defeating to try to deny countries the use of these networks selectively, or to otherwise try to completely isolate the ATI from the wider world.

In addition, the technical knowledge necessary to enable an effective, clandestine attack on the ATI is increasingly common. Solitary hackers and other malefactors have repeatedly demonstrated their ability, often using only the slenderest technical resources, to significantly disrupt U.S. information systems.[27] In 1997 there were 178,856 attempted break-ins to U.S. Army computing systems at the Pentagon building alone, as well as more than 60,000 attacks directed against systems serving the U.S. Air Force and the Office of the Secretary of Defense (OSD).[28] In the same year, computer-related crime resulted in losses of approximately $250 million—a 16 percent increase over 1996.[29] In 1997 more than half of U.S. Fortune 1000 companies reported 30 or more breaches in computer security during the last 12 months; 60 percent of those firms reported losses of $200,000 or more for *each intrusion* [21]. About half the respondents in a 1998 FBI study of computer crime cited the global Internet as the point from which attacks originated; the remainder cited internal corporate networks.[22] Citizens from developing nations represent about 65 percent of all doctoral candidates in computer science studying at U.S. universities [23]. The National Security Agency (NSA) has publicly acknowledged that potential adversaries are developing a body of knowledge about Department

---

[26] *Third Wave warfare* is a concept developed by Drs. Alvin and Heidi Toffler in Ref. 17.

[27] A recently released DOD study pointed out that the information vulnerability faced by the U.S. military is largely a self-created problem: "Program-by-program...we have based critical functions on inadequately-protected telecomputing services. We have created a target-rich environment, [while] U.S. industry has sold globally much of the generic technology which can be used to strike these targets." [Report quoted in Ref. 18.]

[28] According to representatives of the Single Agency Manager (SAM) for Pentagon Information Technology, "most" of these attacks were unsuccessful. See Ref. 19.

[29] Results of a survey of 520 security organizations serving corporations, government agencies, financial institutions, and universities, reported in Ref. 20.

of Defense (DOD) and other U.S. computer systems and about methods to attack these systems [24, p. 4].

As shown in Figure 4, it is easier than ever for even a relatively unsophisticated attacker to exploit systems vulnerabilities via network connections. In the early 1980s, an intruder required a high level of technical knowledge to successfully penetrate computers. By the early 1990s, automated tools for disabling audit software, stealing passwords, and spoofing packets on networks were common. These tools do not require much technical expertise to use. Most have user-friendly Graphical User Interfaces (GUI): automated attacks can be initiated with the simple click of a computer mouse [12, p. 2-15]. One of these tools is WatcherT, a high-technology artificial intelligence engine that is rumored to have been created by a foreign intelligence service [12, p. 2-16]. It is designed to look for several thousand known vulnerabilities in all kinds of computers and networks—including personal computers (PCs), UNIX-based client/server setups, and mainframes.

MG John P. Casciano, Assistant Chief of Staff for Intelligence of the U.S. Air Force, has perhaps said it best: "Actual intrusions into our (military) systems are today relatively benign, mostly at the (individual) hacker level. But, the more people think and talk about computer intrusions...the more folks are going to try their hands at it. The tools of the hacking trade are available over the Internet.... You don't have to know the guts of the computer and

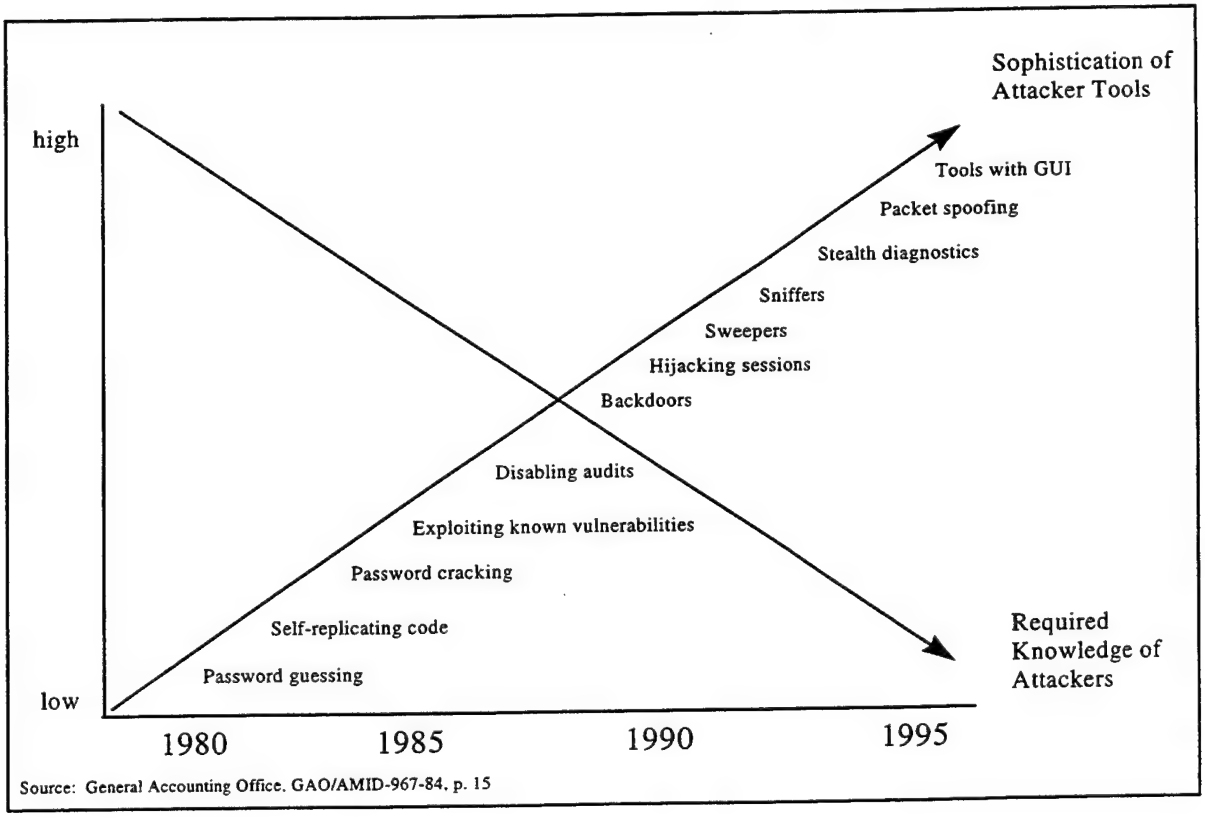

Figure 4. Increase in Sophistication of Hacking Tools.

communication business. You just download the software, point and click, and you, too, can be an Information Warrior [25]."

3.3.3.1 The Hacker Threat: Case Studies

The United States' growing dependence on the routine availability of a networked environment has created opportunities for attackers to interfere with this country's computer operations—both commercial and military. The skills necessary to penetrate U.S. military information systems have been repeatedly demonstrated in nonmilitary arenas. This situation has, in many cases, created a new form of computer mercenary. In other cases of computer network infiltration, however, the motivation of the perpetrator is much more difficult to determine. This section will address two manifestations of the threat of computer network attack: the hacker threat and foreign national computer network attack (CNA) programs.

3.3.3.1.1 Cybersabotage in the Gulf War? During Operations DESERT SHIELD and DESERT STORM (1990-1991), there were a number of media reports of teenage Dutch hackers having offered their services to Iraq for pay. Some 34 U.S. military and nonmilitary government sites did experience a sharp increase in the number of hacking attempts against them beginning soon after the United States began deploying troops to the Gulf region [26, 27]. U.S. officials reportedly learned in October 1990 that the information was being offered to Iraq [28]. Soon after U.S. troops arrived in the Gulf, a computer security trade publication reported that Dutch hackers were systematically searching U.S. military computer systems for specified character strings, including such words as "missile," "weapons," "nuclear," and "Patriot [26]." In February 1991, Dutch television interviewed an unidentified hacker who claimed to have collected "sensitive information" related to Operation DESERT STORM [26].

In late March 1997, Eugene Schultz, a California-based consultant who had worked as manager of a computer security team at the Department of Energy during the Gulf War and helped track the Dutch hackers, revealed that the latter had indeed obtained information that was "...sensitive, but not compromising to the Allied war effort." The Dutch hackers were identified by the FBI but never prosecuted—partly because at that time the Netherlands had no laws prohibiting unauthorized access to computers.[30]

3.3.3.1.2 The Mitnick Case.[31] For almost 16 years, Kevin Mitnick, a U.S. citizen, hacked into U.S. corporate and military-interest computers from various locations inside the United States. Mitnick began his hacking in 1981, with the Pacific Bell Telephone Company as his target. Once he was able to access the telephone network, he would alter subscribers' telephone service, delete data, and modify records to his own financial advantage. In 1983, he was arrested for hacking into computers belonging to the University of Southern California (USC) and TRW Corporation. Later that year, after his release, Mitnick illegally accessed computers belonging to Digital Equipment Corporation and to several telephone companies.

---

[30] Schultz's interview is cited in Ref. 28. Schultz's justification for the U.S. Government's failure to shut off all access by the Dutch hackers is informative: "We couldn't do anything about it," he said. "If we had shut down one machine they were getting into, they would have found others to launch their attacks from....It was one huge mistake to store military secrets on machines connected to the Internet. Information stored on computer is often too accessible to those who shouldn't see it....The 'lesson learned' is to isolate or encrypt information (like this)."

[31] This summary of the Mitnick case is taken from Ref. 29.

Mitnick was aided by his friend Lewis DePayne, and others, beginning around June 1992. Mitnick and his group used both social engineering and "password sniffing"[32] to learn user account identifiers and their corresponding passwords, then used them to access computers that contained proprietary commercial software Mitnick wanted to steal. Mitnick sometimes ran automated hacking programs on the target instead, in order to obtain superuser status on that machine. He routinely stored the proprietary software he stole on the USC computers he had conquered earlier in his career. During the 1994-95 Christmas season, he used IP spoofing techniques to break into the San Diego Supercomputing Center.[33]

On 15 February 1995, Mitnick was finally taken into custody on 25 counts of obtaining unauthorized access to computers and stealing proprietary computer software.[34]

3.3.3.1.3 Datastream Cowboy (the Rome Labs Case).[35] From 23 March to 16 April 1994, two hackers—one a 16-year-old British citizen who went by the nickname "Datastream Cowboy"—attacked computers that supported the U.S. Air Force's premier command-and-control research facility—Rome Laboratory. To make their intrusions more difficult to trace, the hackers wove their way through several international telephone switches to a computer modem in Manhattan. They used Trojan Horses and password sniffing to break into the lab's systems. After more than 150 intrusions, the hackers succeeded in taking all 33 Rome Labs subnetworks off line for several days. In the meantime, they stole sensitive air tasking order (ATO) research. They also launched other attacks from Rome Labs' network, gaining access to systems at NASA's Goddard Space Flight Center, Wright-Patterson Air Force Base, and to various defense contractors around the country.

The pattern of attack was spotted by an alert systems administrator at the Labs. After a brief investigation, Rome Labs' officials notified the Air Force Information Warfare Center (AFIWC) in San Antonio, TX, and the Air Force Office of Special Investigations (AFOSI) in Washington, DC. Working together with system administrators (SYSADs) at Rome Labs, the Air Force officials regained control of the Labs' network. They also monitored the hackers' activities—monitoring which led to the arrest of "Datastream Cowboy" by Scotland Yard.[36]

AFIWC officials estimated that the attacks on Rome Labs cost the U.S. Government over $500,000, including the time spent to investigate the case, take the Labs' systems off the

---

32 "Password sniffers" are computer programs that, when clandestinely installed on a target computer, capture the account information and passwords of authorized users during log in. The hacker then uses that information to reenter the computer in the guise of an authorized user—frequently using an account that has long been inactive (say, the account of an employee who has retired or resigned), but which has not yet been purged from the system.

33 The story of Mitnick's electronic assault on the supercomputing center can be found in Ref. 30.

34 Mitnick was formally charged with violating U.S. Code 1029 (Possession of Unauthorized Access Devices), U.S. Code 1030(a)(4-5) (Computer Fraud), and U.S. Code 1343 (Wire Fraud: Interception of Wire or Electronic Communications). See Ref. 29.

35 This summary of the "Datastream Cowboy" (Rome Labs) incident is taken directly from Ref. 24, pp. 3-4, and Ref. 31.

36 "Datastream Cowboy" (Richard Pryce) was charged with stealing British telephone service—not with breaking into U.S. military computers—and was ultimately sentenced to pay a fine and court costs amounting to 1450 £. His accomplice, Matthew Bevan, was apprehended in mid-1996. See Ref. 32.

network, verify their integrity, install security patches, and restore service. However, this estimate did not include the value of the research data compromised by the hackers. Information is, in general, very difficult to appraise. Rome Labs' officials admitted, however, that Datastream Cowboy might easily have damaged their ATO project beyond repair had he been interested in doing so, and that if this had happened, the research data would have taken some $4 million and 36 months to reconstruct.

3.3.3.1.4 The Argentine Hacker. In 1995 and 1996, a hacker from Argentina used the Internet to illegally access the computing system of a U.S. university. From there, he broke into computers at the Naval Research Laboratory, other DOD installations, NASA, and the Los Alamos National Laboratory. The systems at these sites contained aircraft design, radar technology, and satellite engineering information that is ultimately used in weapons design and C2 systems [24, p. 25].

3.3.3.2 Implications of Hacker Activity

The cases listed here are evidence of an alarming trend toward widespread vulnerability on the part of U.S. military-interest information systems. Of particular concern is what the outcome *might have been* had attacks such as these been coordinated so as to occur simultaneously and/or had the hackers' tools and techniques been employed with more destructive intent. This possibility is the subject of the next section.

3.3.3.3 IW and CNA

Forms of IW are practiced daily by nations, subnational groups—even by corporations. Potential targets of IW attacks can include information, information systems, people, and facilities that support critical information-dependent functions. The means of attack can be both electronic and physical. IW consists not only of *offensive* actions to gain access to someone else's information, but of *defensive* measures taken to protect information as well. The recent increase in interest in IW defensive measures within DOD is in direct response to a heightened awareness of potential IW threats. Finally, IW is adaptive: practitioners of IW learn from their experiences at a rate that has no parallel in other forms of warfare [12, p. 3-2].

Computer network attack is a critical component of offensive IW.

3.3.3.3.1 Potential Adversaries. As U.S. reliance on computers has grown, so has the list of adversaries with the skill to exploit this reliance. CNA offers a veil of anonymity to its potential practitioners. No longer do countries necessarily need to recruit clandestine agents having access to U.S. battle plans or key decisionmakers. All they may need is an anonymous person at a keyboard, with a network connection and the appropriate software. The lack of geographic, spatial, and political boundaries in cyberspace offers further anonymity. While such a "cyberspace agent" does not need to be a highly skilled programmer, such knowledge does provide an advantage. With the rise of graphical user interfaces, many forms of attacks can be launched against systems with only the skills necessary to respond to prompts or to enter data into fields. CNA is relatively cheap to wage as compared to conventional forms of attack, offering a high return on investment to the resource-poor.

3.3.3.3.2 Foreign National CNA Programs. Several countries have CNA programs of relatively long standing. Even more wish to observe the "lessons learned" by others before preparing programs of their own. About 100 countries have some level of active IW program; intelligence sources estimate that about half those programs include the United States among

their targets [33]. As of mid-1996, more than 120 nations were exploring the means for executing remote attacks on a computer network [24, pp. 4-5]. Given these facts, virtually all countries can be seen as *potential* threats to the ATI.

But which countries represent a *current* threat? This question cannot be answered by reference to the largely material indices of the Industrial Age threat once posed to NATO by the Soviet Union and its allies. Rather, threats must be identified by *indirect* means—such as by considering whether a given country possesses most or all of the following:

- CNA Doctrine: A widely agreed set of politico-military objectives and principles meant to guide the employment of CNA resources, and a realized organizational scheme for carrying out a CNA campaign plan. Contrary to popular expectation, a great deal can be learned about the CNA doctrines of most countries by careful examination of open sources.
- State-Sponsored Computer Training Programs designed to prepare information warriors for their tasks.
- A History of CNA Actions.

Perhaps the key factor in assessing whether a nation which otherwise has the technical capability of launching a computer network attack on the ATI (as practically all do) represents an actual "threat" or not is that nation's intention and motivation for attacking.[37] Threat identification is necessarily subjective and, in the CNA world, the constellation of threats is subject to rapid change. A number of nations that currently have little or no interest in CNA could—given sufficient incentive—emerge as major threats to the ATI virtually overnight.

Table 4 provides a sampling of foreign national CNA programs, based on MITRE's analysis of the latest publicly available information. The programs have been subjectively rated according to the four-part threat-identification schema outlined above.

Table 4. Features of Selected Foreign National CNA Programs

COUNTRY	DOCTRINE	TRAINING	HISTORY
China	"Advanced"*	Limited	Limited
France	?	Probable	Substantial
India	Rudimentary	Probable	Limited
Russia	Rudimentary	Probable	Substantial
United States	Advanced	Limited	Limited

*The Chinese appear to have adopted major elements of U.S. IW doctrine wholesale but are working to imbue it with uniquely Chinese characteristics to yield a doctrine that can actually be implemented under Chinese military-economic conditions.

37 A strong industry proponent of this view is information systems security expert Mr. Jim Morris, who is a vice-president of Trident Data Systems Inc., McLean, VA. Morris spoke on the vulnerability of the U.S. National Information Infrastructure (NII) to computer network attack in Ref. 34.

Four of the more extensive foreign CNA programs known to exist are described here.

China's CNA Program. Since 1978, China's gross national product (GNP) has grown at an estimated average rate of 10 percent annually. In January 1997, it commanded the world's second largest reserve of foreign currency ($105 billion) and had a $124 billion foreign trade surplus. It has reportedly been spending a large share of this economic windfall on developing a CNA program [35, p. 469]. Largely as a result of the Gulf War, the Chinese recognize that the mechanized warfare of the Industrial Age had given way to the "five-dimension warfare" characteristic of the Information Age. The resulting military revolution "...is pushing China's units to the crossroads of military reform [36]."

China's information technology (IT) base is growing rapidly. More than 1 million PCs were sold there in 1995, and about 2.7 million in 1996 [37]. Some 300,000 Chinese computers are now connected to the global Internet, up from only 20,000 in 1993. The number of Internet subscribers in China is officially expected to top two million by the end of the century, and seven million in 2001 [38]. According to a recent article by three officers of the People's Liberation Army (PLA) Academy of Electronics Technology, the country's information infrastructure is expected to "...guarantee great advances (not only in) the national economy, (but) in progress in the cause of national defense" through IW [39]. They take it as a given that the IT currently being acquired by China has inherent "dual uses" (civilian and military), and that a large proportion of it will be pressed into service to fight a future information war. China's plans for such a war include a decapitating first strike against the enemy's reconnaissance, surveillance, and communications networks [39].

In the aftermath of Operation DESERT STORM, a frenzy for strategy-related research and writing gripped the Chinese military and military-intellectual communities. As a result, Chinese theorists have apparently concluded that scientific progress has decisively changed the character of warfare and that CNA must be speedily introduced into Chinese military planning. Chinese writers seek to adapt an emergent Western IW theory to the realities of China. They also call on millennia-old but "uniquely Chinese" principles to guide the military in conducting this new type of war. Chinese military scholars have an excellent grasp of the United States' vision, concepts, and organization for information operations. They often parrot our formulations exactly, by way of urging Beijing on which course it should adopt. The Chinese are avid readers of the West's professional military journals and of books by "futurist" visionaries like Drs. Alvin and Heidi Toffler.[38] The Chinese also appear to have adopted elements of Russia's evolving IW doctrine (see below) as their own [40].

The PLA is the chief proponent for military planning in the People's Republic of China (PRC). From the Persian Gulf War, the PLA initially drew the following conclusions relevant to CNA [emphasis added] [36]:

- Along with air raids and other long-distance attacks, information and electronic warfare played a *decisive role* in combat operations, while the ground phase only "enhanced" the results the former had achieved.

---

[38] See Ref. 39. The Tofflers' books *The Third Wave* (Bantam 1980) and *War and Anti-War* (Ref. 17) are largely responsible for popularizing the notions of an Information Age and of information operations, respectively.

- The key targets for attack were the enemy's "brain" and "nervous system," rather than his fighting units.
- There was no clear separation between the front and rear and no distinct battle lines. Operations proceeded in all directions and in depth from the outset of the war.
- *Defense can be accomplished via the offense.*

The PLA also appears to have come to the following insights [41]:

- Army structures will convert from the "material type" to the "information type"; fighting at close quarters will gradually be phased out.
- Reinforcing the CNA capacity of one's own side is the key to a winning victory.
- The development of interconnected networks makes it possible for one to conduct a war from one's own home territory.

The Chinese have officially concluded that a future war cannot be won without inflicting continuous, broad-based CNA attacks on the enemy throughout the conflict (and likely before and after, as well) and that IW is going to be "...small-scale, difficult-to-locate, short...(and) known for multiple and tremendous threats [41]." The Chinese goal in such a war was neatly summarized by scholar Cai Renzhao, in his 1996 article *Exploring Ways to Defeat the Enemy Through Information*:

> "The People's Republic should...seek measures by which to damage the enemy's intelligence-gathering and [data] transmission abilities, and weaken the enemy's information capacity...prior to, or immediately upon, the outbreak of a future war."[39]

On 11 April 1996, the PLA Society for Overall Military Planning announced the formation in Beijing of a think-tank, the Military Strategies Research Center (MSRC). This Center is charged with putting forward strategies for defeating a superior enemy under high-technology conditions, including by means of "...electronic warfare, network warfare, and structural sabotage [42, 43]." In late 1996, the Chinese State Council commissioned a small group of high-level representatives of the military, academic, technical, and banking communities to administer investments in the Chinese NII [40]. The Council took this action partly in recognition of the fact that China, like the United States, relies on its NII to support military communications [40]. In early 1997, the Chinese General Staff established a new IW Department, with the power to coordinate at the national level CNA-related research and strategy formulation, and tactics [44].

Attracted by the cheapness and anonymity of computer network attacks, one of the Chinese strategies appears to be to coordinate the efforts of a large number of ordinary computer users throughout China (and possibly elsewhere) to "...drown our enemies in an ocean of information (as part of an IW) offensive." Such an information-based confrontation would enable the Chinese to reach "...a tangible peace through intangible war...deterring and blackmailing the enemy with (our) dominance in the possession of information [37]." The Chinese appear sincerely to believe that CNA will allow them to implement the "all-conquering stratagem" of the ancient Chinese general Sun Tzu, which claims that by sowing confusion and inhibiting cooperation among the enemy at all levels, a general can "...subdue the enemy without fighting. (This is) the acme of skill [45]."

---

[39] Renzhao was quoted in Ref. 35.

To date, both offensive and defensive elements have been incorporated into the Chinese CNA program. However, the distinctly *offensive and preemptive* nature of the Chinese program comes through clearly in the Chinese' many official and semiofficial writings on the role of information in future conflict [46]. The Chinese believe that measures taken to destroy or degrade an enemy's information systems *effectively guarantee* the unimpeded flow of the Chinese' own information and the establishment of a "transparent battlefield" to be exploited by the Chinese General Staff.[40] The Chinese computer virus development effort is said to be particularly well-funded and technically sophisticated.[41]

A recent book published by the Office of the Director of Net Assessment (DNA) details Beijing's doctrinal shift away from its 50-year-old, low-technology, personnel-intensive military doctrine to one of high-technology regional warfare based on information deterrence and, possibly, "first strikes" aimed at adversary information systems [48]. At the same time, a report published by the House National Security Committee identifies several key technologies China wants to acquire in order to modernize its military. Prominent among these are advanced intelligence, surveillance and reconnaissance capabilities, and enhanced command and control networks [49]. Robert Ellsworth, a former Deputy Secretary of Defense and ambassador to NATO, was quoted as saying in a May 1997 interview that the Chinese can master some of the technologies and methods relevant to CNA within 5-10 years [48]. In early April 1998, all branches of the Chinese Armed Forces reportedly took part in military exercises designed to prepare PLA officers and men to fight "regional wars employing high technology [50]."

Having conducted an exhaustive analysis of the Seven Martial Classics of ancient China and of the Chinese "strategic culture" in general, Harvard political scientist A. I. Johnston has concluded that the Chinese have always stressed the value of violent solutions to security conflicts and the value of offensive over defensive strategies [51]. Noncoercive means are, the Chinese believe, called for only when confronting a more powerful enemy; they are to be used only as an expedient, until China can be sure of prevailing. Johnson contends that lately, China's willingness to use force has grown with the improvement in its military and industrial capacity—and that the country is likely to be even more confrontational as it grows stronger.

In testimony before Congress in early February 1997, Army LTG Patrick M. Hughes (Director, Defense Intelligence Agency) stated that China's military is emphasizing "key force multipliers" including IW, unconventional countermeasures, and tactics [52]. Chang Mengxiong, a leading official at China's Commission on Science, Technology, and Industry for the National Defense (COSTIND), has noted that new weapon types should be judged according to their ability to fill what he called the "information-intensity gap [48]." Wendy Frieman, a Washington, DC-area specialist on the Chinese military, said in a May 1997 interview that China has been "...making decisive progress in software development and other dual use capabilities...

---

[40] See Ref. 35. Most mentions of computer viruses in the Chinese press concern the virus threat to China and specifically identify the United States as the source of the viruses. It is probable that much of this talk actually refers to the results of virus research being performed in China but which is—in typical Chinese fashion—routinely attributed to the "enemy."

[41] Evidence of the Chinese' preccupation with viruses can be found in Ref. 47, especially, pp. 4-5.

If the Chinese decide to [continue investing] in these areas, they have the beginnings of a capability which would support them in achieving their objectives."[42]

Notwithstanding China's significant gains on the CNA front in recent years, however, the state of Chinese preparedness to conduct an IW campaign is still primitive compared with that of the United States. While the U.S. Defense Science Board in November 1996 favorably assessed the quality of Chinese technology available to support *defensive* IW, China was assessed to have only minor or nascent capabilities in areas critical to the conduct of computer network *attack*—such as software and network engineering and means of nonlethal destruction.[43] For now, at least, China continues to acquire most categories of its offensively oriented IW technology abroad.[44] And as Martin Libicki, a leading IW specialist on the faculty of the National Defense University in Washington, DC, said in early 1997, "...militaries, especially those representing widely different cultures, cannot prosper by copying one another. Their endowments, circumstances, and [therefore] strategies differ greatly... We know the Chinese can copy our thoughts, but whether they can innovate in pursuit of their own objectives is not yet obvious."[45] At a symposium organized by the Chinese Electronics Society in Beijing in September 1997, a Chinese analyst probably affiliated with the PLA General Staff Research Institute was quoted as saying that China "...should not deify the power of IW... Compared to countries that are strong in the field of military affairs, the level of defense information modernization in China is currently still relatively backward... (This situation) has the potential to endanger the stability of China's national defense [54]."

The traditional Chinese obsession with secrecy and security; the historical tendency for the momentum to dissipate out from under the Chinese' grand projects; the penchant of Chinese officialdom to revert to passivity following brief bursts of action; and the dead weight of the country's geriatric Communist Party leadership all argue that Chinese progress in realizing their ambitions for CNA will be slower and more uneven than they currently hope it will be. One of the "solutions" to China's backwardness called for by the symposium speaker quoted above, for example, was to "...gradually achieve the nationalization of all computer systems" in the country [54]. While it is very doubtful that confiscation of computers would make the Chinese computing infrastructure any more efficient, this is a typical Chinese Communist approach. Richard Macke, former commander-in-chief of the U.S. Pacific Command (CINC, PACOM), said on 15 May 1997 that he doubted whether China had the technical and industrial capacity to realize many of its ambitions for future warfare, but that Beijing's quest for enhanced military effectiveness via CNA, and other means, is "understandable [53]."

France's CNA Program. The French have been less forthcoming than the Chinese regarding their CNA doctrine and its supporting infrastructure. What is known is that the French entered into the CNA arena early. In 1983, hackers working for the French domestic security

---

[42] Cited in Ref. 53. Ms. Frieman is an employee of Science Applications International Corporation (SAIC), Arlington, VA.

[43] Studies in China have reportedly concluded that in any future conflict with the United States, China's offensive CNA capability would be more important than its defensive capability, simply because the United States depends far more on high-technology information systems than does China. See Ref. 33.

[44] Based on a table appearing in Ref. 12, p. A-12.

[45] Libicki quoted in Ref. 35.

service (*Direction de la Surveillance du Territoire*, or DST) accessed computers both within foreign-owned companies, and outside of French territories. These French-sponsored hackers targeted computers around the world but paid special attention to both national security-related and commercial computer systems in the United States and Great Britain.[46]

Beginning in 1989, the DST ran operations targeting the self-styled Chaos Computer Club, headquartered in Germany, which the DST suspected of trying to hack into computers belonging to the French electronics giants Thomson and Pechiney [55]. As part of this counterintelligence and security effort, the DST set up a "Chaos Computer Club of France (CCCF)" with the express object of meeting would-be hackers, learning their techniques, and sharing detailed vulnerabilities information on the computer systems into which they had hacked.[47]

By early 1997, France had developed a "limited" IW capability. Their program included both defensive and offensive elements and placed priority on recruitment of "controlled" hackers [4]. France's official "technical information warfare center" is the *Centre Electronique de l'Armament* (CELAR). It plays a (presumably advisory) role in every French armament program that might possibly be impacted by developments in CNA [55].

CELAR reportedly devotes about half its work effort to the design of information and communications hardware and to arrangements designed to ensure their security, one-third to the development of electronic and optronic warfare techniques, and the remaining 10 percent to work on encryption technologies. CELAR's 950-strong staff includes 350 military and civilian engineers. CELAR is subordinate to the *Delegation Generale pour l'Armament* (DGA) of the French Ministry of Defense and may enjoy a close working relationship with the French military intelligence service (DRM) [56].

India's CNA Program. According to press reports, in 1996 the Indian Army planned to spend far more on information technology than it had in the previous six years combined. The Army—chief proponent for IW in India—received $3.14 million in its 1996-97 budget earmarked for information technology, compared with less than $2 million for the years 1990-95. Indian Army leaders, however, had requested $20 million [57].

The new money was part of a $45.3 million triservice integrated warfare program, Project SAMYUKTA, which is scheduled to be completed by November 2000 and is intended to accomplish the total overhaul of the Indian military's intelligence gathering, surveillance, jamming, and counterjamming systems.

In press articles that appeared in early 1997, India was listed as having an "advanced" IW program [23]. By contrast with the other countries examined in this section, the U.S. Defense

---

[46] France's best-known computer hacker, Jean-Bernard Condat, went to work for the DST as a teenager after committing a misdemeanor for which he was promised immunity from prosecution if he cooperated. The DST organized his participation in hacker meetings abroad. Condat claims that he broke with the DST in 1991, but that in his 52-month career as a counterintelligence agent he wrote up 1,032 reports. As of October 1995, Condat was the site manager of the *France Forum* on Compuserve (Ref. 55).

[47] See Ref. 55. Jean-Bernard Condat organized the CCCF on behalf of his DST handlers. The DST printed hundreds of T-shirts and thousands of postcards for the "club" to distribute, in an effort to attract the largest possible number of hackers to membership.

Science Board found in November 1996 that India excelled in areas potentially critical to the conduct of computer network *attack*, such as software and network engineering, but had only minor or nascent *defensive* technical capability—namely, in computer and information security. Moreover, the country developed a wide array of both the offensive and defensive technologies it used indigenously, relying on outsiders to supply little [12].

A brief example serves to illustrate one of the uses to which India's emerging CNA capability could be put. Soon after the end of the Gulf War, an Indian Army brigadier advised the leaders of underdeveloped countries that, since they could not hope to take on the U.S. military on the battlefield and win, they should instead be prepared to use computer network attacks to disrupt what he identified as the United States' "Achilles' heel"—namely, our logistics network.[48]

Russia's CNA Program. The Russians have had a lot of experience using electronics in warfare, and the country has what is possibly the oldest CNA program in existence. By 1985, the KGB was employing hackers to access computer networks around the world. The most famous case of this type was documented in Clifford Stoll's book *The Cuckoo's Egg* [16], wherein Dr. Stoll relates his yearlong effort to track down a "wily hacker" who had accessed the computer system Stoll managed at the Lawrence Berkeley Laboratory in Berkeley, CA. The trail led from Berkeley, via the Advanced Research Projects Agency's (ARPA) Military Network (MILNET) and the German public data network, to a West-German hacker who was in the pay of the KGB.

According to extensive media reporting, General Dzhokar Dudayev, president of the breakaway Chechen Republic, was killed as a direct result of Russian IW. In early 1996, an air-launched missile blew to pieces the vehicle next to which Dudayev was standing, while Dudayev was parked in the middle of a farmer's field talking on a commercial satellite telephone.[49] Press speculation has it that the Russians used the signal from the satellite telephone to target Dudayev from a position more than 150 miles away [60]. Although homing in on an ordinary transmitted signal requires neither skill nor sophisticated technology, detecting any such low-powered signal from among background clutter, identifying which specific signal to home in on, and conducting targeting on the basis of this information (in "real time") does.

President Yeltsin's reelection platform (1996) called for the Russian state, among other things, "...to devote more attention to developing the entire range of means of information warfare....[61]" Moreover, even as it drastically cuts outlays on conventional forces, in early 1997, the Russian Parliament doubled defense research and development (R&D) appropriations to $2 billion [62].

The Russian Army believes it is passing from an era in which it assessed the correlation of forces (COF) based mainly on the relative *physical* quantities of combat materiel available to the antagonists to one in which the COF can be practically "read off" from the superior ability of one side or the other to effect precision kills and implant computer viruses [63]. The Gulf War demonstrated to the Russians the "changing ratio" between attack, tactical C2, and information support systems in the accomplishment of combat tasks. Some Russian officers assessed the

---

[48] See Ref. 58, p. 213. When he wrote, Brigadier V.K. Nair (VSM, ret.) was Deputy Director for General Strategic Planning of the Indian Army.

[49] See Ref. 59 as one example of the intense media coverage this event received.

U.S.-led Coalition victory as resulting from an overwhelming superiority not only in logistics, *but in combat and information support systems* [emphasis added].[50] They consider "...the development of superiority in data collection, processing, and presentation such as that seen in the Gulf [to be] a new phenomenon of conflict [64]." To the Russians, IW (*informatsionnoye protivoborstvo*) is a component of "sixth-generation warfare" and effectively erases the line between war and peace. It also adds "another dimension" to the principle of surprise.[51]

In 1995 Russia had 1.2 million personal computers, of which 25 percent had been made in Russia or other states of the former Soviet Union. By 1996 there were some four million computers, almost all of which were imported. There is almost no indigenous software manufacturing in Russia—most offices in government and industry employ IBM PC clones running Windows 95.[52] Russia's efforts to close the "information security gap" they perceive vis-a-vis the United States is hampered by a lack of money to fund research and the fact that many of Russia's best computer scientists are emigrating. The country has therefore adopted a policy of simply trying to control the information threat and to compromise with its most likely practitioners abroad [44].

On the offensive side, the Russians are struggling to develop the capability to disrupt an enemy's information support system. The goal is to forestall his ability to gather, transmit, and process information. Another mission is to "disinform the enemy in every way....[67]" An Information Operations Research Cell is believed to be subordinate to the Russian General Staff Academy [18]. There is also an IW Department at the Russian Institute for Strategic Studies (ISS). Department director, Vladimir Ustinov, told a British reporter in 1996 that "...We have told the [Yeltsin] government that a lot of attention must be paid to information warfare. But, the whole of our military budget is half the amount America spends on [IW] [44]." Beginning in 1991, Russia has devoted especially great attention to attacks using—and ways to defend against—computer viruses [18,68].

In the meantime, leading Russian defense intellectuals—and, probably, the planners they support—are so frightened by the prospect of having a CNA campaign launched against their country in the future that they claim to consider the use of nuclear weapons against the perpetrator(s) to be an appropriate and proportional response. Consider the following irresponsible speech delivered to an international audience by leading Russian IW expert Dr. V. I. Tsymbal, in late 1995:

> "[Given] the possible catastrophic consequences [for Russia] of the use of strategic information warfare by an enemy...Russia retains the right to use nuclear weapons *first* against the means and forces of information warfare, and *then* against

---

[50] See Ref. 64, p. 114, cited in Ref. 63, Note 24.

[51] See Ref. 65. The leading theoretical exponent of "sixth-generation warfare" in Russia is retired Russian General-Major V. Slipchenko, the author of Ref. 66. Russia's leading exponent of computer network attack doctrine is probably Colonel Sergei Modestov of the Russian General Staff (Ref. 40).

[52] See Ref. 44. Russian computer security officials reportedly suspect that many of the PCs being brought to Russia come complete with viruses already imbedded in them "...by the CIA." "We all use Western equipment in our infrastructure—telephones, satellites, computers," said Vitaly Tsygichko, who holds the National Security portfolio on the Russian Federation Council. "These all come from Western firms, and nobody knows what could be hidden inside."

the aggressor state itself....From a military point of view, the use of information warfare means against Russia...will categorically *not* be considered a 'nonmilitary phase' of conflict, whether or not casualties resulted [emphasis added]."[53]

While Russian officers and scholars who have openly addressed the impact of the information revolution on the military do not officially represent the Russian Ministry of Defense (MOD) or General Staff, warnings like Tsymbal's probably closely reflect official thinking in those two beleaguered institutions.

On the other hand, some Russians discount the entire U.S. IW effort as a ruse. A late 1995 article on IW by three Russian academics noted that the U.S. emphasis on IW may be designed, as the Strategic Defense Initiative (SDI) in the 1980s allegedly was, simply to bankrupt the Russian state by encouraging Russia to try to keep up with American "advances" in the field [70].

While a landmark report released by the U.S. Defense Science Board in November 1996 assessed the quality of Russia's *defensive* IW technologies favorably, Russia was assessed to have only minor or nascent capabilities in enabling technologies critical to the conduct of computer network *attack*, such as software and network engineering [12]. Moreover, while most of its security products were home-grown (including computer security devices and programs), Russia relied on foreign acquisition of most of what it had in the engineering realm [12].

3.3.3.3.3 Summary: The IW Threat. In late 1996, the U.S. Defense Science Board published the following information, shown in Table 5, assessing the relative maturity of various IW threats [12, p. 2-12].

By March 1996 DOD had over 2.1 million computers, 10,000 local networks, and 100 long-distance networks. There were over two million DOD computer users and another two million users who did business with DOD [24, p. 10]. However, vulnerability assessments had been performed on less than 1 percent of all DOD computer systems around the world [24, p. 33].

Table 5. IW Threat Estimate

ORIGIN OF THREAT	KNOWN TO EXIST	PROBABLY EXISTS	LIKELY BY 2005	ONLY AFTER 2005
Incompetent User	Widespread			
Hacker	Widespread			
Disgruntled Employee	Widespread			
Domestic Extremists		Widespread		
Terrorist Group		Limited	Widespread	
Foreign Espionage	Limited		Widespread	
Tactical IW Attack			Limited	Widespread
Strategic IW Attack				Limited

[53] See Ref. 69, reported in Ref. 63, p. 1.

As early as 1995, it was estimated that DOD computers were attacked about 250,000 times per year; however, only one in 500 of those attacks was detected and reported. Most DOD computers tested by "controlled" hackers (Red Teams) were easily exploited using "front door" attacks, because even the most basic protections were missing [71; 12, p. 2-15].

U.S. experience in designing highly reliable computer systems does not appear to scale to a large, distributed information infrastructure. Prior R&D efforts have focused on specific areas such as computer and network security, encryption technology, and coping with benign network outages caused by single-node failures. Little attention has been paid to the design and implementation of systems capable of surviving willful, malicious attack. Even less attention has been paid to the process of incorporating legacy systems whose parameters are not under the designers' control.[54]

It is clear that the vulnerability of the U.S. information infrastructure is growing more acute. Not only are more activities becoming dependent on information systems, but these information systems are becoming more open to outsiders and, in the process, adopting technologies that make them less secure (for example, "open" operating systems, Web browsers, and distributed objects). Security technologies are themselves advancing, but the sophistication, availability, and ease of use of hacker tools is advancing faster. Protection is likely to be mostly a matter of operator diligence coupled with the employment of third-party software tools and expertise.

At present most computer systems are vulnerable to information attacks, even if most intrusions are more annoying than dangerous. Yet the frequency of intrusions is rising, and the possibility of a digital Pearl Harbor cannot be dismissed out of hand. Indeed, defense of the nation's information infrastructure is more likely to become an instrument of U.S. national power than offensive information war [72].

As Air Force MG Casciano has said: "Right now much of our unclassified, but nonetheless sensitive information...moves over the commercial communications backbone. [Most of] our critical information in support of military planning and execution runs over commercial links... We have considered encryption and the use of closed systems, but ultimately, we've got to manage the risks [25]."

3.4 Impact

The consequences of any attack on the ATI would fall into one or more of the following categories:

3.4.1 Compromise

Compromise refers to any circumstance or event that may result in loss of confidentiality—that is, in an individual or group gaining access to information they are not authorized to have. Compromise includes the following:

- Exposure: Sensitive or protected information is *directly* released to unauthorized persons.

---

[54] Conclusion of an independent research team affiliated with the Defense Science Board, reported in Ref. 12, Appendix F: *Technology Issues*, p. F-18. See also Ref. 12, p. 3-5.

- Interception: Sensitive or protected data is accessed by unauthorized persons, *while the data is being sent over a communications path.*
- Inference: Unauthorized persons are able to *derive* classified or sensitive information, by reasoning from data that is not classified or sensitive.

3.4.2 Deception

Deception involves the receipt by an authorized user(s) of false information *that is believed to be true*. Deception includes the following:

- Masquerade: An unauthorized individual or entity poses as authorized in order to gain access to the system.
- Falsification: An authorized user is sent false data.
- Repudiation: An individual or entity falsely denies responsibility for some act.

3.4.3 Denial/Loss

Denial/loss refers to the disruption of an information system's services and functions, thus potentially preventing the system from fulfilling its mission. Denial/loss includes the following:

- Corruption: System services are interrupted by the adverse modification of a critical function or piece of data.
- Obstruction: Service is interrupted due to the saturation *(flooding)* of system functions or controls by excessive amounts of information or numbers of commands.
- Destruction: Destruction (sometimes called *incapacitation*) refers to any action in which system operation is prevented or interrupted due to the disabling of critical system components.
- Theft of computing services.

3.4.4 Situation-Dependent Impact

Impact is determined by the operational context in which the damage occurs. For example, a denial of service or compromise of information that might prove devastating to a commander on the battlefield might well be almost trivial when that same commander's forces are out of contact with the enemy—and vice versa. The loss of a server handling purely administrative matters—personnel reenlistment statistics, and the like—for a tank battalion will be of understandably small import to that battalion's commander at the moment his turrets are turning to face the enemy. At that same moment, however, the corruption of a server responsible for updating enemy position data could prove decisive.

Ultimately, then, each commander must decide for him- or herself the value of a particular type of information in a given setting—and thus the potential impact of the degradation or loss of the information system that carries it. Arriving at a calculus of impact based on the relative value of different types of information in different operational settings appears to be a very fruitful area for further work.

3.5 Safeguards

The number and variety of safeguards relevant to computing and communications systems like the ATI is great indeed. The relative effectiveness of various safeguards is beginning to receive the detailed attention of DOD research and testing laboratories, contractors, universities, and the computer-hobbyist community. For this reason, only two of the most common classes of safeguards will be discussed here.

3.5.1 Tactics, Techniques, and Procedures (TTP)

Improvements in TTP can serve as an effective and relatively inexpensive safeguard against at least the most common types of computer-based threats to Army information systems like the ATI. Enhancing TTP could mean upgrading some or all of the following:

- Tools
- Training
- Operator awareness
- Testing (including the institution of "Red Teaming")
- Employment of integrated security mechanisms

3.5.2 Computer Emergency Response Teams (CERTs)

Computer Emergency Response Teams (CERTs) receive reports of the unauthorized disclosure of data, denials of service, and inadequate system response times, which have potentially serious implications for tactical combat elements. CERTs are maintained by each of the U.S. military services, by government agencies, and by at least one multinational body.

In June 1997, the U.S. Army established an Army Computer Emergency Response Team Coordination Center (ACERT/CC) in the offices of the Intelligence and Security Command (INSCOM), Fort Belvoir, VA, to coordinate the Army's response to attacks on its computer systems and information networks. With an FY 1997 budget of about $1.7 million, the ACERT/CC is chartered to keep track of attacks on Army computer networks and information systems and, when required, to provide guidance to field commanders on how to identify potential saboteurs, fix damaged or compromised systems, and prevent further attacks.

The ACERT/CC is intended to work closely with the Army's regional CERTs (called RCERTs), as well as with the Defense Information Systems Agency's (DISA's) Automated Systems Security Incident Support Team (ASSIST)—the Pentagon's lead computer security response organization—and the computer security centers of the other military services. There is already one RCERT in Germany; the Army plans to stand up one at Fort Huachuca, AZ, as well as one or possibly two in the Pacific in FY 1998 [73].

The U.S. Air Force CERT is maintained at Kelly Air Force Base, San Antonio, TX. Its Navy counterpart resides at the Fleet IW Center in Norfolk, VA. The federal CERT/CC is managed by the Software Engineering Institute at Carnegie-Mellon University, Pittsburgh, PA. Several other countries with CERTs[55] have joined the United States in forming the Forum of Incident

[55] Germany, the Netherlands, Switzerland, and Australia.

Response and Security Teams (FIRST). The National Institute of Standards and Technology (NIST), headquartered in Gaithersburg, MD, currently serves as secretariat for the FIRST.

In its November 1996 study, the Defense Science Board rated "...the capability to conduct independent technical assessments of the vulnerabilities inherent in DOD computing and communications systems" as one of the "top five" capabilities necessary for effective, defensive IW [12, p. 6-3, Exhibit 6-2]. The most robust organization from an IW defense perspective would be one which was a totally independent auditing agency, with the capability to detect state-sponsored CNA conducted with the active collusion of an authorized insider, based on testing and examination of both accidents and the responses from a live contingency-planning exercise designed to simulate a specified assessment scenario.[56] Two other needs pointed out by the Board were the need for realistic threat assessments and for security-enhancing improvements in system, network, and infrastructure design practices [12].

3.6 Assessing Risk

Risk is defined as the relative degree of exposure of an asset (as, the ATI and the information it carries) to damage given the prevailing combination of vulnerabilities, threats, operational impact, and safeguards. The following five tables, taken together, represent an attempt to express in qualitative terms the risk faced by computer and communications networks like the ATI arising from various types of threats. This exercise is based on what is probably the most common risk-assessment methodology in the computer security and financial communities [74, pp. 616-624].

First, Table 6 provides examples of the types of damage that might be inflicted on the ATI by various parties—witting or unwitting.

Second, we can characterize the likelihood of damage based upon the *average frequency* with which it can be expected to occur, and—if the damage is the result of a deliberate attack—the *level of skill required* of the perpetrator(s) to invoke the damage. This is shown in Table 7.

Table 8 characterizes the *impact* of a given incident, based on the damage inflicted.

Next, Table 9 arrives at a characterization of *overall risk*, based on Impact and Likelihood.

Finally, Table 10 assigns these levels of risk to specific types of threats.

---

[56] This conclusion was arrived at by a research team affiliated with the Defense Science Board. The team's unofficial results were reported in Ref. 12, p. C-2.

Table 6. Threats and Associated Damage

ORIGIN OF THREAT	EXAMPLES(S) OF DAMAGE
Unauthorized Access	
Allies	Access to data outside of need to know Destruction or corruption of data
Neutrals	Access to data Destruction or corruption of data
Enemies	Access to data Destruction or corruption of data and files Loss of system to network control (battle overrun)
Authorized Access	
Browsing	Access to data outside of job function
User Error	Destruction or corruption of data or file systems Compromise of password controls/other security procedures
Administrator Error	Compromise of password controls/other security procedures
Other	
Malicious Software	Access to data (Trojan Horse) Destruction or corruption of data (viruses, worms) Loss of trust in system
System Failure	Loss of data

Note: "Other" threats to ATI systems include battle damage, damage in transport, etc. However, the types of physical protection required to counter these threats is beyond the scope of this analysis and are not addressed here.

Table 7. Characterizing the Likelihood of Damage

FREQUENCY/SKILL LEVEL REQUIRED	LIKELIHOOD OF DAMAGE
Occurs less than once per year, OR Requires conspiracy and/or system designer-level knowledge	Rare
Occurs a few times per year, OR Requires single user with SYSAD-level knowledge and access	Infrequent
Occurs on average once per month No special skills or access required	Routine
Occurs on average once or more per week No special skills or access required	Frequent

Table 8. Characterizing Impact

DAMAGE	IMPACT
Violation of need-to-know principle Minor loss/corruption of data Loss of service less than 1 hr	Negligible
Moderate loss/corruption of data Loss of service 1-6 hr	Marginal
Human lives endangered Extensive loss/corruption of data Loss of service more than 6 hr Users question system's further utility	Critical
Loss of life Loss of system Complete loss/corruption of data Complete loss of trust in the affected (and similar) systems	Catastrophic

NOTE: The equation of damage and impact is made here only for the purposes of arriving at a generalized risk assessment, with a view toward illustrating the logical steps by which a full-bodied, system-specific risk assessment would be conducted. As stated in Section 3.4 above, impact is actually determined by the operational context in which the damage occurs and is thus a much more complex phenomenon than can be captured in Table 8.

Table 9. Overall Risk

IMPACT	LIKELIHOOD			
	Rare	**Infrequent**	**Routine**	**Frequent**
Negligible	Low	Low	Moderate	Moderate
Marginal	Low	Moderate	Moderate	High
Critical	Moderate	Moderate	High	Extreme
Catastrophic	Moderate	High	High	Extreme

Table 10. Risk Arising From Specific Types of Threats

ORIGIN OF THREAT	IF LIKELIHOOD =	AND IMPACT =	THEN RISK =
Unauthorized Access			
Allies	Infrequent	Negligible	Low
Neutrals	Infrequent	Marginal	Moderate
Enemies	Infrequent	Critical	Moderate
Authorized Access			
Browsing	Frequent	Negligible	Moderate
User Error	Routine	Marginal	Moderate
Administrative Error	Infrequent	Critical	Moderate
Other			
System Failure	Frequent	Marginal	High
Malicious Software	Infrequent	Catastrophic	High

Ideally, once threats are identified, safeguards should be applied in sufficient quantity and with the degree of sophistication necessary to reduce all risks to low. It is a rule of thumb among systems engineers that under no circumstances should high or extreme risks be carried into the production phase [15]. Moderate risks represent a "gray area" in which the application of safeguards will depend on the time and money available and the criticality of the mission performed by the systems potentially affected by an attack or malfunction.

INTENTIONALLY LEFT BLANK.

4. Conclusions and Recommendations

4.1 Conclusions

The United States and other technically advanced nations are especially vulnerable to computer network attacks, since these nations rely heavily on today's electronic communications and data-exchange technology. An adversary can attack information backbones with little investment in talent and equipment, yet these attacks can cause catastrophic system failures and loss of life.

Computer networks are potentially highly vulnerable to intrusion, for reasons which include the following:

- Attacks can originate from anywhere on the globe via the commercial Internet.
- Technically advanced equipment is available to anyone (friend or foe).
- Attackers can employ any number of readily available, sophisticated software "hacking tools," such as Watcher-T, which drastically lower the skill level needed to launch a successful remote attack.
- Many computer systems are not aggressively managed and are poorly equipped to protect against intruders.

Understanding vulnerabilities is the key to managing risk.

Investment in safeguards should be commensurate with overall risk. One should therefore endeavor to estimate the overall risk arising from each identified threat before procuring such safeguards.

The ATI's networked environment potentially exposes each of its component systems to the security weaknesses characteristic of any one component, *plus* additional weaknesses inherent in the network itself. However, a common architecture also makes possible the provision of common security features, at minimum cost.

While attacks by lone hackers are the most common being experienced today, sponsored attacks stand a much greater chance of doing severe damage to the ATI and of harming the U.S. military operations, which depend upon its availability and reliability. State-sponsored programs for computer network attack represent the greatest near-term threat to the ATI.

The U.S. military's ability to respond to computer emergencies in an organized fashion and on a large scale has made a promising start but is still in its infancy. Sensitive but unclassified military-interest computer systems and networks are essentially unprotected at other than the local level. In many cases, such systems are "indirectly" connected to classified systems.

4.2 Recommendations

Given these facts, a commitment is clearly warranted to develop the means for information protection, countermeasures against attack, communications alternatives, and reliable recovery modes. Reasonable steps must be taken to minimize the Army's current vulnerability. In general, the Army should commit resources to ensure that ATI systems are appropriately

protected, their security posture is aggressively managed, and the systems are carefully operated to reduce to an acceptable level the risks to the Army's mission and forces.

The Army should move immediately to increase awareness of the overall risk posed to the ATI, assess ATI dependencies and vulnerabilities, and "raise the bar" with high-payoff, low-cost "fixes" for existing vulnerabilities. Such "patches" must be both technical and procedural, in recognition of the vital part human factors engineering plays in security operations and administration.

The Army should closely monitor the progress of commercial information technologies. As cost-affordable technologies are developed by the market, they should be given early tests to determine their suitability for employment by Army tactical forces—especially as part of a rapidly assembled system in the Joint or Coalition environments, which are the Army's future. The Army should establish a commercial off-the-shelf (COTS) information system technology evaluation capability to identify vulnerabilities and find the nullifying modifications, to help the Army be an informed buyer, and to provide risk assessment and advisory services to both current users and system developers.

Finally, the Army should focus R&D for the future and provide adequate resources to ensure that the ATI is as secure and as survivable as possible for a given expenditure. Army R&D funds should be focused on those aspects of information assurance and protection that are NOT likely to be addressed by the private sector. Such R&D programs must emphasize cost and operational realism. Army R&D programs should focus on the following areas:

- Robust, survivable system architectures.
- Tools and techniques for the automated detection and analysis of information attacks (both localized and large-scale).
- Test beds and simulation-based mechanisms for evaluating emerging technologies and tactics of potential use in defending Army information systems.
- Modeling of tactical C4I systems and their critical components and resources, and simulating their modes of failure.

The Army should require that vulnerability and countermeasures analysis be conducted on any new system during the R&D phase. It should continue to seek to demonstrate the effectiveness of survivable architectures experimentally, in both existing technology test beds and in those still to emerge. A comprehensive, unified R&D effort, similar to earlier investments that established U.S. preeminence in cryptography, may be required to correct shortcomings in the current Army R&D effort.[57]

---

57 This last was the conclusion of an independent research team affiliated with the Defense Science Board, reported in Ref. 12, Appendix F: *Technology Issues*, p. F-18. See also Ref. 12, p. 3-5.

5. References

1. U.S. Department of Defense. *Quadrennial Defense Review, 1996.*
2. U.S. Army Training and Doctrine Command (TRADOC). *Force XXI Operations: Army Vision XXI.* TRADOC Pamphlet 525-5, Fort Monroe, VA., updated 13 March 1998. http://www.tradoc.army.mil/pubs/maps/p525-5cg.htm
3. U.S. Department of the Army. *Operations.* FM 100-5, June 1997. http://www.atsc-army.org/cgi-bin/atdl.dll/fm/100-5/100-5toc.htm
4. Thompson, Mark. "Wired for War." *TIME*, p. 72, 31 March 1997.
5. Edwards, Sean J. A. "The Threat of High-Altitude Electromagnetic Pulse to Force XXI." *National Security Studies Quarterly*, Vol. III, Issue 4 (Georgetown University), Autumn 1997.
6. Fourth Quarterly Conference of the U.S. Army Information Operations Intelligence Working Group (IOIWG), Fort Monmouth, NJ, 5-6 February 1998.
7. Burk, R. et al. *TCP/IP Blueprints,* Section 2.4, Indianapolis, MN: Sam's Publishing, 1997.
8. Melford, Bob. "TCP/IP Limitations Undone." *SunWorld*, January 1997.
9. Army Missile Defense Modernization page of the U.S. Army Air Defense (ADA) School, Fort Bliss, TX, updated 9 December 1997. http://147.71.152.73/amd/html/Chapter-5.htm
10. "Joint Technical Architecture-Army (JTA-A)." Version 5.0, 11 September 1997. http://www.hqda.army.mil/techarch/jtaa50/jtaa50.htm
11. Defense Information Systems Agency (DISA). http://www.itsi.disa.mil/
12. Report of the Defense Science Board Task Force on Information Warfare—Defense (IW-D). Appendix A, *Threat Assessment*, November 1996.
13. U.S. Army Digitization Office (ADO). February 1997.
14. U.S. Army Digitization Office. *Master Plan* coordination draft, Fall 1996. http://www.ado.armymil/ADMP/1996/TOC.htm
15. Banning, Charles. Personal communication. MITRE Institute Professional Development Course TSE100, 12 January 1998.
16. Stoll, Clifford. *The Cuckoo's Egg: Inside the World of Computer Espionage.* New York: Doubleday, 1989.
17. Toffler, Alvin, and Heidi Toffler. *War and Anti-War.* New York: Warner Books, 1993.
18. Bellamy, Christopher. "Britain's Defences Down Against Cyber-Warriors." *The Independent* (London), p. 14, 13 March 1997.
19. *Defense News.* 3 March 1998. http://web.lexis-nexis.com/more/cahners-chicago/11407/3065318/9>
20. *San Francisco Chronicle.* 4 March 1998. http://web.lexis-nexis.com/more/cahners-chicago/11407/3065318/5>

21. "WarRoom Research LLC." *Internet Week*, 23 March 1998.

22. Study by the Computer Security Institute and U.S. Federal Bureau of Investigation (FBI). *Internet Week*, 23 March 1998.

23. Valeri, Lorenzo. "Guarding Against a New Digital Enemy." London *Sunday Times*, Features, 16 March 1997.

24. General Accounting Office (GAO). "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks." AIMD-96-84, May 1996.

25. Casciano, John P. Untitled speech to the Los Angeles Foundation Forum, 18 October 1996. http://www.aef.org/la9.html

26. Alexander, Michael. "Hackers Find 'Open Season' on Internet." *Computerworld*, p. 8, 29 April 1991.

27. Academy of Criminal Justice Sciences. "Trends and Experiences in Computer-Related Crime." 1996.

28. Statement by Eugene Schultz in the documentary *Sci Files*, aired by BBC-TV on 24 March 1997, reported in "TV Documentary Says Dutch Hackers Stole Gulf War Secrets," *AP Worldstream*, 24 March 1997.

29. *United States vs. Kevin David MITNICK*, indictment file CR 96-881, February 1995.

30. Shimomura, Tsutomu, and John Markoff. *Takedown: The Pursuit and Capture of America's Most Wanted Computer Outlaw—By The Man Who Did It.* Hyperion, January 1996.

31. U.S. Senate, Permanent Subcommittee on Investigations (Minority Staff Statement). "Security in Cyberspace." Appendix B (Case Study: Rome Laboratory/Griffiss Air Force Base, NY), Intrusion, Washington, D.C., 5 June 1996.

32. Gold, Steve. "U.S. Defense Hacker Case: Datastream Cowboy Fined." London: Newsbytes, 21 March 1997.

33. Wilson, J. R. "Waging the InfoWar." *Jane's International Defense Review*, Vol. 2, No. 4 (Extra), p. 1, 1 April 1997.

34. Georgetown University Symposium. "National Security in the Information Age: Issues, Challenges, and Capabilities." 15 November 1997.

35. Ahrari, M. Ehssan. "Chinese Prove to be Attentive Students of Information Warfare." *Jane's Intelligence Review (Asia),* Vol. 9, No. 10, 1 October 1997.

36. *"Extremely Important" Meeting of Central Military Commission*, Kuang Chiao Ching' no. 280, Hong Kong, in Chinese, 16 January 1996, pp. 6-10. Trans. in BBC Summary of World Broadcasts, Part 3 (Asia-Pacific/China, Internal Affairs), 9 February 1996.

37. Wei, Jincheng. *New Form of People's War*, Jiefangjun Bao, in Chinese, 25 June 1996, p. 6., trans. as *Information Warfare With Chinese Characteristics*, FBIS-CHI-96-159, 16 August 1996.

38. Golden, William, citing the China Xinhua News Agency. "China Has 620,000 People Surfing the Internet." *National Military Intelligence Association (NMIA) Z-Gram*, 16 March 1998.

39. Wang, Su, and Zhang. "Untitled," Jisuanji Shijie [*China Computerworld*], no. 30, in Chinese, 11 August 1997, p. 21, trans. as *China: Information Revolution, Defense Security*, FBIS-CHI-97-324, 20 November 1997.

40. Holt, Taylor. Personal communication. Military Technology Division, U.S. Army National Ground Intelligence Center (NGIC), Charlottesville, VA, 17 December 1997.

41. *China: Characteristics of Information Warfare Explored*, Jiefangjun Bao, Beijing, in Chinese, 16 April 1996, trans. in BBC Summary of World Broadcasts, Part 3 (Asia-Pacific/China, Military), 10 May 1996.

42. *Army Establishes Strategic Research Center*, BBC Summary of World Broadcasts (Part III/Asia-Pacific, Military), 1 August 1996, trans. of Chinese People's Liberation Army newspaper Jiefangjun Bao, in Chinese, 21 May 1996.

43. *PRC Establishes Psy-, Info-War Centre*, Defense and Foreign Affairs/Strategic Policy, p. 3, 31 August 1996.

44. Adams, James. "Anoraks' Apocalypse." *Sunday Times*, Features, 16 March 1997.

45. Sun Tzu. *The Art of War* (Samuel B. Griffith, trans.), Oxford University Press, 1963.

46. Wang, Su, and Zhang. "Untitled," Jisuanji Shijie [*China Computerworld*], no. 30, in Chinese, 11 August 1997, trans. as *China: Information Revolution, Defense Security*, FBIS-CHI-97-324, 20 November 1997.

47. Zhu, Xiaoning. *Counter-Computer Electronic Warfare*, Xiandai Bingqi [Modern Weaponry] no. 10, October 1995, trans. by the U.S. Army National Ground Intelligence Center, Charlottesville, VA, as *Electronic Warfare Directed Against Computers*, NGIC-HT-0211-96, 17 April 1996.

48. U.S.GPO/Office of the Secretary of Defense/DNA. *Chinese Views of Future Warfare*, ed. Michael Pillsbury, 1997.

49. National Security Committee, U.S. House of Representatives, 1997. "Selected Military Capabilities of the People's Republic of China." *American Intelligence Journal*, Vol. 17, Nos. 3 & 4, p. 96, Autumn 1997.

50. China Xinhua News Agency. "Army Drills for High-Tech Warfare." *Inside China*, Reuters News Agency, 14 April 1998, cited in *National Military Intelligence Association (NMIA) Z-Gram*, 15 April 1998.

51. Johnston, Alastair Iain. *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*, Princeton University Press, October 1995.

52. Hughes, Patrick M. "Statement for the Senate Select Committee on Intelligence (5 February 1997) and Senate Armed Services Committee (6 February 1997)," found on the Infowar.com WWW site. *wysiwyg://119/* http://www.infowar.com/mil_c4i/mil_c4izd.html-ssI.

53. Opall, Barbara. "Chinese Covet High-Technology Arsenal." *Army Times*, 19 May 1997.

54. Dai Kouhu. "Accepting the Challenge: Reinforcing China's Defense Information Modernization." *China Electronics News*, p. 8, Beijing, 24 October 1997, in Chinese, trans. in FBIS DIW, 12 January 1998.

55. Indigo Publications. "A Computer Spy Unmasked." *Intelligence Newsletter* No. 273, 12 October 1995.

56. Indigo Publications. "France Advances on Infowar Front." *Intelligence Newsletter* No. 289, 6 June 1996.

57. Raghuvanshi, Vivek. "Indian Army Hikes Info Tech Funding." *Defense News*, p. 8, 28 October-3 November 1996.

58. Nair, V. K. *War in the Gulf: Lessons for the Third World*, New Delhi: Lancer International Press, 1991.

59. *Chechen: U.S. Helped Kill Dudayev*, UPI International, 2 October 1996.

60. Muradian, Vago. "Russians Killed Chechen Leader With Precision-Guided Missile." *Defense Daily,* Vol. 195, No. 25, 5 May 1997.

61. *Text of Yeltsin's Election Programme*, BBC Summary of World Broadcasts, Part 1 (Former USSR); Special Supplement EE/D2636/S1, 13 June 1996.

62. Crock, Stan. "We Will Cyber-Bury You." *Business Week,* No. 3523, p. 6, 21 April 1997.

63. Thomas, Tim. *Russian Views on Information-Based Warfare*, Foreign Military Studies Office (FMSO), Fort Leavenworth, KS, July 1996. http://leav-www.army.mil/fmso/opart/pubs/airpower.htm

64. Lebedev, Lyutov, and Nazarenko. "War in the Persian Gulf: Lessons and Conclusions." *Military Thought,* No. 11-12, in Russian, December 1991.

65. Vladimirov, A. "Information Weapons: Myth or Reality?" *Red Star*, in Russian, 5 October 1991.

66. Slipchenko, V. "Analysis of Warfare Leading to the 6th Generation." *Field Artillery*, October 1993.

67. Vayner, A. Ya. "On Opposition in the Sphere of Command and Control." *Military Thought,* No. 9, in Russian, pp. 18-23, September 1990, trans. in JPRS-UMT-90-009-L, pp. 10-13, 21 November 1990.

68. Modestov, Sergei. *At the Invisible Front: Warfare Activization*, Delovoy Mir [Business World], in Russian, p. 7, 24 February 1994.

69. Tsymbal, V. I. *Concept of Information Warfare*, speech delivered to the U.S.-Russian Conference on Evolving Post-Cold War National Security Issues (Moscow, 12-14 September 1995), in Russian.

70. Smolyan, Tsygichko, and Chereshkin. *A Weapon That May Be More Dangerous Than a Nuclear Weapon: Realities of Information Warfare*, Nezavisimaya Gazeta (Supplement), No. 3, in Russian, 18 November 1995, pp. 1-2, trans. in FBIS-UMA-95-234-S, pp. 31-35, 6 December 1995.

71. DISA briefing. "Developing the Information Warfare Defense: A DISA Perspective," December 1995.

72. National Defense University. "Strategic Assessment 1996." Ch. 15: *Emerging Military Instruments*, pp. 10-12, 1996. http://www.infowar.com/mil_c4i/book/sa96ch15.html-ssi

73. Armed Forces Newswire Service. "Army Stands Up Computer Security Coordination Center," 11 June 1997. *wysiwyg://125/* http://www.infowar.com/mil_c4i/mil_c4iz8.html-ssi

74. Summers, Rita C. *Secure Computing: Threats and Safeguards,* New York: McGraw-Hill, 1997.

INTENTIONALLY LEFT BLANK.

Glossary

ABCS	Army Battle Command System
ACERT/CC	Army Computer Emergency Response Team Coordination Center
ADA	Army Air Defense
Adj BNS	adjacent battalions
ADO	Army Digitization Office
AFATDS	Army Field Artillery Tactical Data System
AFOSI	Air Force Office of Special Investigations
AFIWC	Air Force Information Warfare Center
AMDWS	Air and Missile Defense Workstation
AMPS	Aviation Mission Planning System
ANBACIS	Automated Nuclear/Biological Information System
ARL	(U.S.) Army Research Laboratory
ARPA	Advanced Research Projects Agency
ASAS	All-Source Analysis System
ASAS-RWS	All-Source Analysis System Remote Workstation
ASSIST	Automated Systems Security Incident Support Team
ATA	Army Technical Architecture
ATCCS	Army Tactical Command and Control System
ATI	Army Tactical Internet
ATM	Asynchronous Transfer Mode
ATO	air tasking order
AWE	Advanced Warfighting Experiment
AWIS	Army WWMCCS Information System
BADD	Battlefield Awareness Data Dissemination
BDE	brigade
BN	battalion
BOS	battlefield operating system
C2	command and control
C4I	command, control, communications, computers, and intelligence
CCCF	Chaos Computer Club of France
CELAR	*Centre Electronique de l'Armament* (France)
CERT	Computer Emergency Response Team
CERT/CC	Computer Emergency Response Team Coordination Center
CIA	Central Intelligence Agency
CINC	commander-in-chief
CNA	computer network attack
CNR	combat net radio
COF	correlation of forces
COP	common operational picture
COSTIND	(China's) Commission on Science, Technology, and Industry for the National Defense

COTS	commercial off-the-shelf
CPX	command post exercise
CSMA	Carrier Sense Multiple Access
CSSCS	Combat Service Support Control System
CTIL	Commander's Tracked Items List
DBS	Direct-Broadcast Satellite
DGA	*Delegation Generale pour l'Armament* (France)
DII COE	Defense Information Infrastructure Common Operating Environment
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DNA	Director of Net Assessment
DOD	Department of Defense
DRM	French military intelligence service
DST	*Direction de la Surveillance du Territoire* (France)
EBC	Embedded Battle Command
e-mail	electronic mail
EPLRS	Enhanced Position Location Reporting System
EXFOR	Experimental Force
FAAD	Forward Area Air Defense
FAADC3I	Forward Area Air Defense Command, Control, Communications, and Intelligence
FBCB2	Force XXI Battle Command Brigade and Below
FBI	Federal Bureau of Investigation
FDR	Future Digital Radio
FIRST	Forum of Incident Response and Security Teams
FMSO	Foreign Military Studies Office
FRAGO	fragmentary order
FTP	File Transfer Protocol
FTX	field training exercise
GAO	General Accounting Office
GCCS	Global Command and Control System
GCCS-A	Global Command and Control System, Army
GNP	gross national product
GPS	Global Positioning System
GUI	Graphical User Interface
HF	high-frequency
I&W	indications and warning
ICMP	Internet Control Message Protocol
ID	identifier

IMETS	Integrated Meteorological System
INC	Internet Controller
INSCOM	Intelligence and Security Command (U.S. Army)
IP	Internet Protocol
IPB	Intelligence Preparation of the Battlespace
IPv6	IP Version 6
ISS	Institute for Strategic Studies
ISSO	Information Systems Security Officer
IT	information technology
IW	information warfare
JTA	Joint Technical Architecture
JTA-A	Joint Technical Architecture-Army
KGB	Former Soviet intelligence and security service
LAN	local area network
LEO	low earth orbit
MCS	Maneuver Control System
MCS/P	Maneuver Control System/Phoenix
MHF	manpack high-frequency (radio)
MILNET	Military Network
MILSTAR	(U.S). Military Strategic and Tactical Relay Satellite System
MOD	Ministry of Defense
MSE/TPN	Mobile Subscriber Equipment/Tactical Packet Network
MSG	(EPLRS) Multisource Group
MSRC	Military Strategies Research Center
NFS	Network File System
NGIC	National Ground Intelligence Center
NII	National Information Infrastructure
NIPRNET	Unclassified (but Sensitive) Internet Protocol Routing Network
NIS	Network Information Service
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTC	National Training Center
NTDR	Near-Term Digital Radio
OPFOR	opposing force
OPORD	operations order
OSD	Office of the Secretary of Defense
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First

PACOM	(U.S.) Pacific Command
PC	personal computer
PLA	People's Liberation Army
PRC	People's Republic of China
R&D	research and development
RCERT	Regional Computer Emergency Response Team
RMA	Revolution in Military Affairs
RWS	Remote Workstation
SA	situational awareness
SAIC	Science Applications International Corporation
SAM	Single Agency Manager
SATCOM	satellite communications
SDI	Strategic Defense Initiative
SINCGARS	Single Channel Ground-Air Radio System
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
STACCS	Standard Theater Army Command and Control System
SUID	Superuser Identifier
SYSAD	system administrator
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol and Internet Protocol
TELNET	Telecommunications Network
TFTP	Trivial File Transfer Protocol
TOC	Tactical Operations Center
TTP	tactics, techniques, and procedures
TTY	teletypewriter
UAV	unmanned aerial vehicle
UID	user identifier
U.S.	United States
USC	University of Southern California
UTO	unit task organization
UUDECODE	User-to-User Decode
VMF	Variable Message Format
WAN	wide-area (computer) network
WIN-T	Warfighter Network, Terrestrial
WWMCCS	Worldwide Military Command and Control System

NO. OF COPIES ORGANIZATION

2 DEFENSE TECHNICAL
INFORMATION CENTER
DTIC DDA
8725 JOHN J KINGMAN RD
STE 0944
FT BELVOIR VA 22060-6218

1 HQDA
DAMO FDQ
D SCHMIDT
400 ARMY PENTAGON
WASHINGTON DC 20310-0460

1 OSD
OUSD(A&T)/ODDDR&E(R)
R J TREW
THE PENTAGON
WASHINGTON DC 20301-7100

1 DPTY CG FOR RDE HQ
US ARMY MATERIEL CMD
AMCRD
MG CALDWELL
5001 EISENHOWER AVE
ALEXANDRIA VA 22333-0001

1 INST FOR ADVNCD TCHNLGY
THE UNIV OF TEXAS AT AUSTIN
PO BOX 202797
AUSTIN TX 78720-2797

1 DARPA
B KASPAR
3701 N FAIRFAX DR
ARLINGTON VA 22203-1714

1 NAVAL SURFACE WARFARE CTR
CODE B07 J PENNELLA
17320 DAHLGREN RD
BLDG 1470 RM 1101
DAHLGREN VA 22448-5100

1 US MILITARY ACADEMY
MATH SCI CTR OF EXCELLENCE
DEPT OF MATHEMATICAL SCI
MAJ M D PHILLIPS
THAYER HALL
WEST POINT NY 10996-1786

NO. OF COPIES ORGANIZATION

1 DIRECTOR
US ARMY RESEARCH LAB
AMSRL D
J W LYONS
2800 POWDER MILL RD
ADELPHI MD 20783-1145

1 DIRECTOR
US ARMY RESEARCH LAB
AMSRL DD
J J ROCCHIO
2800 POWDER MILL RD
ADELPHI MD 20783-1145

1 DIRECTOR
US ARMY RESEARCH LAB
AMSRL CS AS (RECORDS MGMT)
2800 POWDER MILL RD
ADELPHI MD 20783-1145

3 DIRECTOR
US ARMY RESEARCH LAB
AMSRL CI LL
2800 POWDER MILL RD
ADELPHI MD 20783-1145

ABERDEEN PROVING GROUND

4 DIR USARL
AMSRL CI LP (305)

NO. OF COPIES ORGANIZATION

1 OUSD AT STRT TAC SYS
DR SCHNEITER
RM 3E130
3090 DEFENSE PENTAGON
WASHINGTON DC 20310-3090

1 ASST SECY ARMY RESEARCH
DEVELOPMENT ACQUISITION
SARD ZP ROOM 2E661
103 ARMY PENTAGON
WASHINGTON DC 20310-0103

1 ASST SECY ARMY RESEARCH
DEVELOPMENT ACQUISITION
SARD ZS ROOM 3E448
103 ARMY PENTAGON
WASHINGTON DC 20310-0103

1 OADCSOPS FORCE DEV DIR
DAMO FDZ
ROOM 3A522
460 ARMY PENTAGON
WASHINGTON DC 20310-0460

1 OADCSOPS FORCE DEV DIR
DAMO FDW
RM 3C630
460 ARMY PENTAGON
WASHINGTON DC 20310-0460

1 ARMY TRNG & DOCTRINE COM
ATCD B
FT MONROE VA 23561-5000

1 ARMY TRADOC ANL CTR
ATRC W
MR KEINTZ
WSMR NM 88002-5502

1 ARMY RESEARCH LABORATORY
AMSRL SL
PLANS AND PGMS MGR
WSMR NM 88002-5513

1 ARMY RESEARCH LABORATORY
AMSRL SL E
MR SHELBURNE
WSMR NM 88002-5513

NO. OF COPIES ORGANIZATION

ABERDEEN PROVING GROUND

1 ARMY TEST EVAL COM
AMSTE TA
APG MD 21005-5055

1 US ARMY EVAL ANALYSIS CTR
CSTE EAC MR HUGHES
4120 SUSQUEHANNA AVE
APG MD 21005-3013

1 US ARMY EVAL ANALYSIS CTR
CSTE EAC SV DR HASKELL
4120 SUSQUEHANNA AVE
APG MD 21005-3013

1 ARMY RESEARCH LABORATORY
AMSRL SL
DR WADE
APG MD 21005-5068

2 ARMY RESEARCH LABORATORY
AMSRL SL B
MS SMITH
W WINNER
APG MD 21005-5068

1 ARMY RESEARCH LABORATORY
AMSRL SL E
DR STARKS
APG EA MD 21010-5423

NO. OF COPIES	ORGANIZATION
1	DEPUTY CHIEF OF STAFF INTELLIGENCE DAMI ST LTC BECKWORD THE PENTAGON WASHINGTON DC 20310-1001
1	OASD C3I DR GONTAREK RM 3E194 6000 DEFENSE PENTAGON WASHINGTON DC 20301-6000
1	HQ INSCOM LIWA STEVE SHANAHAN 8825 BEULAH ST FT BELVOIR VA 22060
1	HQ INSCOM LIWA MS MEHAN 8825 BEULAH STREET FT BELVOIR VA 22060-5246
1	XVIII AIRBORNE CORPS G6 AUTOMATION CPT STEVE BATES 2 1127 A MACOMB ST RM 214 FT BRAGG NC 28314
9	US ARMY RESEARCH LAB AMSRL SL EI MR NOWAK MR MEINCKE MR BARNES MR LURSKI MR LUMA MR MASCIULLI MR BOTHNER MR AMARAL MR JERSCHKOW FT MONMOUTH NJ 07703-5602
2	US ARMY RESEARCH LAB AMSRL IS DR GANTT LTC WALCZAK 2800 POWDER MILL RD ADELPHI MD 20783-1197
7	US ARMY RESEARCH LAB AMSRL SL EA MR FLORES MR LANDIN MS SMITH MR MCDONALD MR NIX MR GUZIE MR STAY WSMR NM 88002-5513
10	US ARMY RESEARCH LAB AMSRL SL EM MR PALOMO MR OCHOA MR ZARRET MR CUELLAR MR PAYAN MR ANDERSON MR HUNT MR ESCUDERO DR DAVENPORT MR HEMMINGWAY WSMR NM 88002-5513
8	US ARMY RESEARCH LAB AMSRL SL EI DR MORRISON MS CHRISTIANSON MR MAREZ MR WILLIAMS MR MCDONALD MS JIMENEZ MR SWEARINGEN SGT GOWINS WSMR NM 88002-5513
2	US ARMY RESEARCH LAB AMSRL SL ET MS THOMPSON DR YEE WSMR NM 88002-5513
1	COMMANDER NGIC AING SBE MR TERRY 220 SEVENTH ST NE CHARLOTTESVILLE VA 22902-5396

NO. OF COPIES	ORGANIZATION
1	LTC B MALONEY 235 B BARNARD LOOP WEST POINT NY 10996
10	THE MITRE CORPORATION MAIL STOP W967 MR HAWORTH 1820 DOLLEY MADISON BLVD MCLEAN VA 22102-3481
1	SYSTEM SECURITY ENGRG TEAM CRUSADER UNITED DEFENSE DR TED LEE 4800 EAST RIVER RD FRIDLEY MN 55421-1498
	ABERDEEN PROVING GROUND
2	US ARMY EAC CSTE EAC SV DR HASKELL MR MYERS
92	DIR USARL AMSRL SL DR WADE MR BEILFUSS AMSRL SL B MR SANDMEYER MS SMITH AMSRL SL BA MS RITONDO MR VOGEL MS JUARASCIO MR HENRY AMSRL SL BE MR BELY MR PETTY MR LINDELL MR SIVACK MR MANYAK DR WEISS

NO. OF COPIES	ORGANIZATION
	AMSRL SL BG MS YOUNG MR FRANZ MR KUSS DR LIU MR PLOSKONKA MR ZIGLER MR GANGLER MAJ POWERS AMSRL SL BN MR FARENWALD MR SMITH MS KUCINSKI MR RUTH AMSRL SL E DR STARKS AMSRL SL EA MR MORRISEY AMSRL SL EI MR PANUSKA (10 CPS) MR ZUM BRUNNEN (50 CPS) AMSRL SL EM DR FEENEY AMSRL SL ET MR BAYLOR MR GARRETT MR NEALON

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	October 1998	Nov 97 - Apr 98

4. TITLE AND SUBTITLE

Analyzing Threats to Army Tactical Internet Systems

5. FUNDING NUMBERS

C: DAAB07-98-C-E601

6. AUTHOR(S)

Robert L. Haworth

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

MITRE Corporation
1820 Dolley Madison Boulevard
ATTN: Dept G045, MS W-967
McLean, VA 22102-3481

8. PERFORMING ORGANIZATION REPORT NUMBER

MTR 98W0000070

9. SPONSORING/MONITORING AGENCY NAMES(S) AND ADDRESS(ES)

U.S. Army Research Laboratory
ATTN: AMSRL-SL-EI
Aberdeen Proving Ground (EA), MD 21010-5423

10.SPONSORING/MONITORING AGENCY REPORT NUMBER

ARL-CR-423

11. SUPPLEMENTARY NOTES

Point of contact for this report Richard L. zum Brunnen, U.S. Army Research Laboratory, ATTN: AMSRL-SL-EI, Aberdeen Proving Ground (EA), MD 21010-5423.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The risk faced by the Army Tactical Internet (ATI) is a function of four elements: vulnerabilities, threats, operational impact, and safeguards (countermeasures). It is clear that the vulnerability of the U. S. information infrastructure is growing more acute. Not only are more activities becoming dependent on information systems, but these information systems are becoming more open to outsiders and, in the process, adopting technologies that make them less secure. Security technologies are themselves advancing, but the sophistication, availability, and ease of use of hacker tools is advancing faster. The consequences of any attack on the ATI include the *compromise of* information, *deception*, and *denial/loss*. Impact is determined by the operational context in which the damage occurs. The degree of potential damage to ATI systems will guide operational users, in conjunction with materiel developers, in selecting appropriate safeguards. The number and type(s) of safeguards employed should balance operational integrity, systems security, and cost concerns in a risk-managed environment.

14. SUBJECT TERMS	15. NUMBER OF PAGES
tactical internet, computer security, hackers, vulnerability	63
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

INTENTIONALLY LEFT BLANK.

USER EVALUATION SHEET/CHANGE OF ADDRESS

This Laboratory undertakes a continuing effort to improve the quality of the reports it publishes. Your comments/answers to the items/questions below will aid us in our efforts.

1. ARL Report Number/Author ARL-CR-423 (Haworth [zum Brunnen]) Date of Report October 1998

2. Date Report Received _____

3. Does this report satisfy a need? (Comment on purpose, related project, or other area of interest for which the report will be used.) _____

4. Specifically, how is the report being used? (Information source, design data, procedure, source of ideas, etc.) _____

5. Has the information in this report led to any quantitative savings as far as man-hours or dollars saved, operating costs avoided, or efficiencies achieved, etc? If so, please elaborate. _____

6. General Comments. What do you think should be changed to improve future reports? (Indicate changes to organization, technical content, format, etc.) _____

CURRENT ADDRESS

_____
Organization

_____
Name E-mail Name

_____
Street or P.O. Box No.

_____
City, State, Zip Code

7. If indicating a Change of Address or Address Correction, please provide the Current or Correct address above and the Old or Incorrect address below.

OLD ADDRESS

_____
Organization

_____
Name

_____
Street or P.O. Box No.

_____
City, State, Zip Code

(Remove this sheet, fold as indicated, tape closed, and mail.)

(DO NOT STAPLE)